FortiOS™ Handbook

Install and System Administration for FortiOS 5.0

Install and System Administration for FortiOS 5.0

January 04, 2016

01-502-142188-20130423

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log

Date	Change Description
2016-01-04	Added missing line for FortiManager configuration
	Added jumbo frames support on FG-100D series.
2014-04-09	Updated the “FortiCloud” chapter.
2014-03-12	Added note to “Entering text strings (names)”.
2014-03-07	Added CAPWAP to “Interface configuration and settings”. Added “Probing Interfaces” section. Edits throughout the document to bring the content up to date for 5.0.6.
2014-02-10	Added a note to “System Resources widget”. Updated “Interface MTU packet size” section.
2013-12-05	Added “Differences between Models and Firmware”, updated “SNMP get command syntax”, updated “Using grep to filter get and show command output”.
2013-09-17	Added “Detection during update”.
2013-09-11	Added: “Change Log,” “Advanced Threat Protection Statistics widget,” “Features widget,” “Adding and removing options from lists,” “Feature Select”, “FortiCloud”. Edits throughout the document to bring the content up to date for 5.0.4.

Chapter 1 Install and System Administration for FortiOS 5.0

This guide contains the following sections:

Differences between Models and Firmware highlights key differences that exist between FortiGate models and firmware versions.

Using the web-based manager provides an overview of the web-based manager interface for FortiOS. If you are new to the FortiOS web-based manager, this chapter provides a high level overview of how to use this method of administration.

Using the CLI provides an overview of the command line interface (CLI) for FortiOS. If you are new to the FortiOS CLI, this chapter provides a high level overview of how to use this method of administration.

Basic Administration describes the simple setup requirements an administrator should do to get the FortiGate unit on the network and enabling the flow of traffic.

Best practices discusses methods to make the various components of FortiOS more efficient and offers suggestions on ways to configure the FortiGate unit.

FortiGuard discusses the FortiGuard network services and configuration examples.

FortiCloud discusses the FortiCloud hosted security management and log retention service.

Interfaces describes the FortiGate interface options and configuration choices.

Central management describes how to configure the FortiGate unit to use FortiManager as a method of maintaining the device and other features that FortiManager has to facilitate the administration of multiple devices.

Monitoring describes various methods of collecting log data and tracking traffic flows and tends.

VLANs discusses the implementation of virtual local area networks (VLANs) in FortiOS and how to configure and use them.

PPTP and L2TP describes these virtual private network (VPN) types and how to configure them.

Session helpers describes what session helpers are and how to view and configure them.

Advanced concepts describes more involved administrative topics to enhance network security and traffic efficiency.

Differences between Models and Firmware

This section examines some of the key differences that exist between different FortiGate models and different versions of the FortiOS 5.0 firmware. It is important to keep these differences in mind when reading the FortiOS 5.0 Handbook, in order to understand how the documentation relates to your specific FortiGate unit.

Differences between Models

- There are certain features that are not available on all models. For example, the Switch Controller, which allows a FortiGate unit to manage a FortiSwitch unit, is only available on FortiGate models 100D, 140D, 200D, 240D, 600C, 800C, and 1000C.

  Other features may be available only through the CLI on models, while other models have options in the web-based manager. For example, SSL content inspection is a CLI-only feature on FortiGate models 20C, 30C, and 40C, while models 60C+ have options in the web-based manager.

  For more information about some of the features that vary by model, please see the Feature/Platform Matrix.
- Naming conventions may vary between FortiGate models. For example, on some models the interface used for the local area network is called *lan*, while on other units it is called *internal*.
- Menus may vary by model. For example, on some FortiGate units, the menu option *Router* is not available. Instead, routing is configured by going to *System* > *Network* > *Routing.*

Differences between Firmware Versions

- Many changes are introduced in new patches to the FortiOS 5.0 firmware. For more information about these changes, please see *What's New for FortiOS 5.0* and the FortiOS *Release Notes*.
- In FortiOS 5.0 Patch 3, *Feature Select* was added, which controls which menus are visible in the web-based manager. If a feature you wish to use does not appear in the web-based manager, go to *System* > *Config* > *Features* to ensure that the feature has not been turned off.
- Menu names may change between firmware versions. For example, In FortiOS 5.0 Patch 3, the features formerly known *UTM Security Profiles* was renamed *Security Profiles*.
- Menus may move between firmware versions. For example, in FortiOS Patch 5, Endpoint Control moved from being part of the *User* menu to having a menu option of its own, found at *User & Device* > *Endpoint Protection.*
- Options may also be removed in a firmware patch. For example, in FortiOS Patch 5, the *Client Reputation Monitor* was removed. Client Reputation results can now be found in the *Threat History* widget.

Using the web-based manager

This section describes the features of the web-based manager administrative interface (sometimes referred to as a graphical user interface, or GUI) of your unit. This section also explains common web-based manager tasks that an administrator does on a regular basis.

The following topics are included in this section:

Web-based manager overview

The web-based manager is a user-friendly interface for configuring settings and managing the FortiGate unit. Accessing the web-based manager is easy and can be done by using either HTTP or a secure HTTPS connection from any management computer, using a web browser.

The recommended minimum screen resolution for properly displaying the web-based manager is 1280 by 1024. Some web browsers do not correctly display the windows within the web-based manager interface. Verify that you have a supported web browser by reviewing the Knowledge Base articles: Microsoft Windows web browsers supported by Fortinet products web-based manager (GUI) web browsers and Mac OS browsers for use with Fortinet hardware web-based manager (GUI).

The web-based manager also provides the CLI Console widget, which enables you to connect to the command line interface (CLI) without exiting out of the web-based manager.

Web-based manager menus and pages

The web-based manager provides access to configuration options for most of the FortiOS features from the main menus. The web-based manager contains the following main menus:

System	Configure system settings, such as network interfaces, virtual domains, DHCP and DNS services, administrators, certificates, High Availability (HA), system time, set system options and set display options on the web-based manager.
Router	Configure static, dynamic and multicast routing and view the router monitor.
Policy	Configure firewall policies, protocol options and Central NAT Table.
Firewall Objects	Configure supporting content for firewall policies including scheduling, services, traffic shapers, addresses, virtual IP and load balancing.
Security Profiles	Configure antivirus and email filtering, web filtering, intrusion protection, data leak prevention, application control, VOIP, ICAP and Client Reputation.

VPN	Configure IPsec and SSL virtual private networking.
User & Device	Configure user accounts and user authentication including external authentication servers.This menu also includes endpoint security features, such as FortiClient configuration and application detection patterns.
WAN Opt. & Cache	Configure WAN optimization and web caching to improve performance and security of traffic passing between locations on your wide area network (WAN) or from the Internet to your web servers.
WiFi & Switch Controller	Configure the unit to act as a wireless network controller, managing the wireless Access Point (AP) functionality of FortiWiFi and FortiAP units.
Log & Report	Configure logging and alert email as well as reports. View log messages and reports.
Current VDOM	Appears only when VDOMs are enabled on the unit to switch between VDOMs.

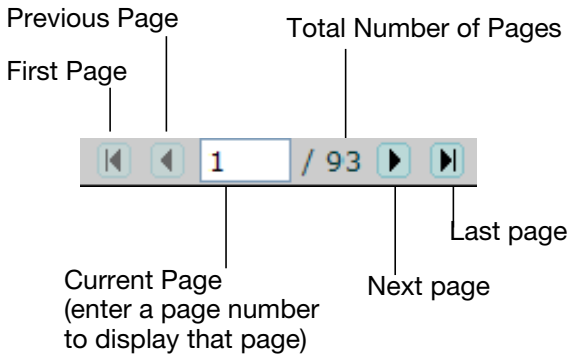
Using information tables

Many of the web-based manager pages contain tables of information that you can filter to display specific information. Administrators with read and write access can define the filters.

Using page navigation

Some pages contain information and lists that span multiple pages. At the bottom of the page is the page navigation controls that enables you to move between pages.

Figure 1: Page controls



Adding filters to web-based manager lists

Filters are used to locate a specific set of information or content within multiple pages. These are especially useful in locating specific log entries. The specific filtering options vary, depending on the type of information in the log.

To create a filter, select *Filter Settings* or the filter icon in a column heading. When a filter is applied to a column, the filter icon becomes green. Filter settings are stored in the unit's configuration and will be maintained the next time that you access any list for which you have added filters.

Filtering variables can include: a numeric range (such as 25-50), an IP address or part of an address or any text string combination, including special characters.

Note that the filtering ignores characters following a “<“ unless the followed by a space. For example, the filtering ignores `<string` but not `< string`. Filtering also ignores matched opening and closing (`<` and `>`) characters and any characters between them. For example, filtering will ignore `<string>`.

For columns that contain only specific content, such as log message severity, a list of terms is provided from which options can be selected.

Using column settings

Column settings are used to select the types of information which are displayed on a certain page. Some pages have a large amounts of information is available and not all content can be displayed on a single screen. Also, some pages may contain content that is not of use to you. Using column settings, you can display only that content which is important to your requirements.

To configure column settings, right-click the header of a column and select *Column Settings*. Any changes that you make to the column settings of a list are stored in the unit’s configuration and will display the next time that you access the list.

To return a page’s columns to their default state, select *Reset All Columns*, located at the bottom of the *Column Settings* menu.

Entering text strings

The configuration of a FortiGate unit is stored in the FortiOS configuration database. To change the configuration, you can use the web-based manager or CLI to add, delete, or change configuration settings. These changes are stored in the database as you make them.

Individual settings in the configuration database can be text strings, numeric values, selections from a list of allowed options, or on/off (enable/disable) settings.

Entering text strings (names)

Text strings are used to name entities in the configuration. For example, the name of a firewall address, administrative user, and so on. You can enter any character in a FortiGate configuration text string except, to prevent Cross-Site Scripting (XSS) vulnerabilities, the following characters:

“ (double quote), & (ampersand), ' (single quote), < (less than) and > (greater than)

Most web-based manager text string fields make it easy to add an acceptable number of characters and prevent you from adding the XSS vulnerability characters.

There is a different character limitation for VDOM names and hostnames. For both, the only legal characters are are numbers (0-9), letters (a-z, A-Z), and special characters - and _.

From the CLI, you can also use the `tree` command to view the number of characters that are allowed in a name field. For example, firewall address names can contain up to 64 characters. When you add a firewall address to the web-based manager, you are limited to entering 64

characters in the firewall address name field. From the CLI you can enter the following `tree` command to confirm that the firewall address `name` field allows 64 characters.

```
config firewall address
  tree
  -- [address] --*name (64)
               |- subnet
               |- type
               |- start-ip
               |- end-ip
               |- fqdn (256)
               |- cache-ttl (0,86400)
               |- wildcard
               |- comment (64 xss)
               |- associated-interface (16)
               +- color (0,32)
```

The `tree` command output also shows the number of characters allowed for other firewall address name settings. For example, the fully-qualified domain name (`fqdn`) field can contain up to 256 characters.

Entering numeric values

Numeric values set various sizes, rates, numeric addresses, and other numeric values. For example, a static routing priority of 10, a port number of 8080, or an IP address of 10.10.10.1. Numeric values can be entered as a series of digits without spaces or commas (for example, 10 or 64400), in dotted decimal format (for example the IP address 10.10.10.1) or, as in the case of MAC or IPv6 addresses, separated by colons (for example, the MAC address 00:09:0F:B7:37:00). Most numeric values are standard base-10 numbers, but some fields (again, such as MAC addresses) require hexadecimal numbers.

Most web-based manager numeric value fields make it easy to add the acceptable number of digits within the allowed range. CLI help includes information about allowed numeric value ranges. Both the web-based manager and the CLI prevent you from entering invalid numbers.

Enabling or disabling options

If a configuration option can only be on or off (enabled or disabled), the web-based manager presents a check box or other control that can only be enabled or disabled. From the CLI you can set the option to `enable` or `disable`.

Dashboard

The various dashboard menus provides a way to access information about network activity and events, as well as configure basic system settings. You can easily add more dashboards and edit existing ones to easily view the content you need.

Each information “chunk” is found within a widget. Widgets provide an easy and quick way to view a variety of information, such as statistical information or network activity. There are a selection of widgets to choose from by selecting the *Widgets* option.

Administrators must have read and write privileges for adding and configuring dashboards and widgets.

Adding dashboards and widgets

Dashboards that you create are automatically added under the default status and usage dashboards. You can add, remove, or rename a dashboard, regardless of whether it is default. You can also reset the Dashboard menu to its default settings by selecting *Reset Dashboards*.

If VDOMs are enabled, only the dashboards within Global are available for configuration.

To add a dashboard

1. Go to *System* > *Dashboard* > *Status*.
2. Select *Dashboard*, located at the top left of the page.
3. Select *Add Dashboard*.

To add a widget to a dashboard, select *Widget* located at the top left of the dashboard page.

System Information widget

The *System Information* widget shows status information on the FortiGate unit and provides the access point to update the firmware and backup the configurations.

Host Name	The name of the FortiGate unit. For details on changing the name, see Changing the FortiGate unit's host name. If the FortiGate unit is in HA mode, this information is not displayed.
Serial Number	The serial number of the FortiGate unit. The serial number is specific to that FortiGate unit and does not change with firmware upgrades.
Operation Mode	The current operating mode of the FortiGate unit. A FortiGate unit can operate in NAT mode or Transparent mode. Select *Change* to switch between NAT and transparent mode. For more information, see Changing the operation mode. If virtual domains are enabled, this field shows the operating mode of the current virtual domain. The Global System Status dashboard does not include this information.
HA Status	The status of High Availability (HA) within the cluster. Standalone indicates the FortiGate unit is not operating in HA mode. Active-Passive or Active-Active indicate the FortiGate unit is operating in HA mode. Select *Configure*, to change the HA configuration.
Cluster Name	The name of the HA cluster for this FortiGate unit. The FortiGate unit must be operating in HA mode to display this field.
Cluster Members	The FortiGate units in the HA cluster. Information displayed about each member includes host name, serial number, and whether the FortiGate unit is a primary (master) or subordinate (slave) FortiGate unit in the cluster. The FortiGate unit must be operating in HA mode with virtual domains disabled to display this information.
Virtual Cluster 1 **Virtual Cluster 2**	The role of each FortiGate unit in virtual cluster 1 and virtual cluster 2. The FortiGate unit must be operating in HA mode with virtual domains enabled to display this information.

System Time	The current date and time. Select *Change*, to configure the system time. For more information, see Configuring system time.
Firmware Version	The version of the current firmware installed on the FortiGate unit. Select *Update* to upload a different firmware version. For more information, see Changing the firmware.
System Configuration	The time period of when the configuration file was backed up. Select *Backup* to back up the current configuration. For more information, see Backing up the configuration. To restore a configuration file, select *Restore*. For more information, see Restoring your firmware configuration.
Current Administrator	The number of administrators currently logged into the FortiGate unit. Select *Details* to view more information about each administrator that is currently logged in If you want to changed the current administrator's password, see Changing the currently logged in administrator's password.
Uptime	The time in days, hours, and minutes since the FortiGate unit was started or rebooted.
Virtual Domain	Status of virtual domains on your FortiGate unit. Select *Enable* or *Disable* to change the status of virtual domains feature. If you enable or disable virtual domains, your session will be terminated and you will need to log in again.
Explicit Proxy Load Balance	The status of each feature. Select *Enable* or *Disable* to change the status of the feature. When enabled, the menu option appears.

Changing the FortiGate unit's host name

The host name appears in the *Host Name* row, in the *System Information* widget. The host name also appears at the CLI prompt when you are logged in to the CLI and as the SNMP system name.

To change the host name on the FortiGate unit, in the *System Information* widget, select *Change* in the *Host Name* row. The only administrators that can change a FortiGate unit's host name are administrators whose admin profiles permit system configuration write access. If the FortiGate unit is part of an HA cluster, you should use a unique host name to distinguish the FortiGate unit from others in the cluster.

Changing the operation mode

FortiGate units and individual VDOMs can operate in NAT or Transparent mode. From the *System Information* dashboard widget, you can change the operating mode for your FortiGate unit or for a VDOM and perform sufficient network configuration to ensure that you can connect to the web-based manager in the new mode.

NAT mode

In NAT mode, the FortiGate unit is visible to the network that it is connected to and all of its interfaces are on different subnets. Each interface that is connected to a network must be configured with an IP address that is valid for that subnet.

You would typically use NAT mode when the FortiGate unit is deployed as a gateway between private and public networks (or between any networks). In its default NAT mode configuration,

the FortiGate unit functions as a router, routing traffic between its interfaces. Security policies control communications through the FortiGate unit to both the Internet and between internal networks. In NAT mode, the FortiGate unit performs network address translation before IP packets are sent to the destination network.

For example, a company has a FortiGate unit as their interface to the Internet. The FortiGate unit also acts as a router to multiple subnets within the company. In this situation, the FortiGate unit is set to NAT mode and has a designated port for the Internet, wan1, with an address of 172.20.120.129, which is the public IP address. The internal network segments are behind the FortiGate unit and invisible to the public access, for example port 2 has an address of 10.10.10.1. The FortiGate unit translates IP addresses passing through it to route the traffic to the correct subnet or to the Internet.

Transparent Mode

In transparent mode, the FortiGate unit is invisible to the network. All of its interfaces are on the same subnet and share the same IP address. To connect the FortiGate unit to your network, all you have to do is configure a management IP address and a default route.

You would typically use the FortiGate unit in transparent mode on a private network behind an existing firewall or behind a router. In transparent mode, the FortiGate unit also functions as a firewall. Security policies control communications through the FortiGate unit to the Internet and internal network. No traffic can pass through the FortiGate unit until you add security policies.

For example, the company has a router or other firewall in place. The network is simple enough that all users are on the same internal network. They need the FortiGate unit to perform application control, antivirus, intrusion protection, and similar traffic scanning. In this situation, the FortiGate unit is set to transparent mode. The traffic passing through the FortiGate unit does not change the addressing from the router to the internal network. Security policies and security profiles define the type of scanning the FortiGate unit performs on traffic entering the network.

To switch from NAT to transparent mode

1. From the *System Information* dashboard widget select *Change* beside *Operation Mode*.
2. From the *Operation Mode* list, select *Transparent*.
3. Enter the *Management IP* address and Netmask. This is the IP address to connect to when configuring and maintaining the device.
4. Enter the *Default Gateway*.
5. Select *OK*.

To change the transparent mode management IP address

1. From the *System Information* dashboard widget select *Change* beside *Operation Mode*.
2. Enter a new IP address and netmask in the *Management IP*/*Network* field as required and select *OK*.

Your web browser is disconnected from the web-based manager. To reconnect to the web-based manager browse to the new management IP address.

To switch from transparent to NAT mode

1. From the *System Information* dashboard widget select *Change* beside *Operation Mode*.
2. From the *Operation Mode* list, select *NAT*.
3. Enter valid IP address and netmask for the network from which you want to manage the FortiGate unit.
4. Select the interface to which the Interface IP/Netmask settings apply
5. Enter the IP address default gateway required to reach other networks from the FortiGate unit.

6. After the FortiGate unit switches to NAT mode, you may need to go *Router* > *Static Route* and edit this default route.

   For low-end FortiGate units, go to *System* > *Network* > *Routing*.
7. Select *OK*.

Configuring system time

The FortiGate unit's system time can be changed using the *System Information* widget by selecting *Change* in the *System Time* row.

System Time	The current system date and time on the FortiGate unit.
Refresh	Update the display of the FortiGate unit's current system date and time.
Time Zone	Select the current system time zone for the FortiGate unit.
Set Time	Select to set the system date and time to the values.
Synchronize with NTP Server	Select to use a Network Time Protocol (NTP) server to automatically set the system date and time. You must specify the server and synchronization interval. FortiGate units use NTP Version 4. For more information about NTP see http://www.ntp.org.
Server	Enter the IP address or domain name of an NTP server. To find an NTP server that you can use, see http://www.ntp.org.
Sync Interval	Specify how often the FortiGate unit should synchronize its time with the NTP server.
Enable NTP Server	Select to make the FortiGate unit an NTP server that client computers can ping for time synchronization. When selected, the Listen on Interfaces option appears. Add the interfaces the FortiGate unit will listen for time requests.

Daylight savings time is enabled by default. You can disable daylight savings time using the CLI commands:

```
config system global
  set dst disable
end
```

Changing the firmware

To avoid losing configuration settings you should always back up your configuration before changing the firmware image.

Also, when updating firmware, you should first refer to *Supported Upgrade Paths for FortiOS Firmware* to help ensure a successful upgrade.

Administrators whose admin profiles permit maintenance read and write access can change the FortiGate unit's firmware. Firmware images can be installed from a number of sources including a local hard disk, a local USB disk, or the FortiGuard Network.

To change the firmware, go to *System* > *Dashboard* > *Status* > *System Information* widget and select the *Update* link on the *Firmware Version* row.

Upgrade From	Select the firmware source from the drop down list of available sources.
Firmware Version	This appears only when selecting *FortiGuard Network* is selected from the *Upgrade From* drop-down list. Select a firmware version from the drop-down list. If downgrading the firmware on the FortiGate unit, select the check box beside Allow Firmware Downgrade.
Upgrade File	Browse to the location of the firmware image on your local hard disk. This field is available for local hard disk and USB only.
Allow Firmware Downgrade	Select to confirm the installation of an older firmware image (downgrade). This appears only when selecting *FortiGuard Network* is selected from the *Upgrade From* drop-down list.
Upgrade Partition	The number of the partition being updated. This field is available only if your FortiGate unit has more than one firmware partition.
Boot the New Firmware	By default, this is enabled. Select to disable the FortiGate unit's reboot process when installing a firmware image to a partition. This option enables you to install a firmware image to a partition without the FortiGate unit rebooting itself and making the firmware image the default firmware that is currently running.

You need to register your FortiGate unit with Customer Support to access firmware updates for your model. For more information, go to http://support.fortinet.com or contact Customer Support.

Backing up the configuration

Administrators can back up the FortiGate unit's configuration file from the *System Information* widget. Select *Backup* in the *System Configuration* row, to back up the firmware configuration file to a local computer, USB disk or to a FortiManager unit.

You should always back up your configuration whenever you make any modifications to the device configuration or performing any firmware updates or changes.

Local PC	Select to back up the configuration file to a local management computer.
FortiManager	Select to back up the configuration file to a FortiManager unit. The Central Management settings must be enabled and a FortiManager unit connected with the FortiGate unit so that the FortiGate unit can send the configuration file to the FortiManager unit. To enable central management, go to *System* > *Admin* > *Settings*.

USB Disk	Select to back up the configuration file to a USB key that is connected to the FortiGate unit.
Full Config	Select to backup the full VDOM configuration. This appears only when the FortiGate unit has VDOM configuration enabled.
VDOM Config	Select to backup the only the VDOM configuration file. This option backs up only the configuration file within that VDOM. Select the VDOM from the drop-down list, and select *Backup*.
Encrypt configuration file	Select to enable a password to the configuration file for added security.
Password	Enter the password that will be used to restore the configuration file.
Confirm	Re-enter the password.

Formatting USB

The FortiGate unit enables you to back up the configuration of the device to a USB flash drive. The USB flash drive must be formatted as a FAT16 disk.

To formate the USB flash drive, either use the CLI command `exe usb-disk format`. or within Windows at a command prompt, enter the command

```
format <drive_letter>: /FS:FAT /V:<drive_label>
```

where *<drive_letter>* is the letter of the connected USB flash drive and `<drive_label>` is the name to give the USB drive.

Remote FortiManager backup and restore options

After successfully connecting to the FortiManager unit from your FortiGate unit, you can back up and restore your configuration to and from the FortiManager unit.

A list of revisions is displayed when restoring the configuration from a remote location. The list allows you to choose the configuration to restore. To use the FortiManager unit as a method of backup and restore of configuration files, you must first configure a connection between the two devices. For more information, see Central management.

Remote FortiGuard backup and restore options

Your FortiGate unit can be remotely managed by a central management server that is available when you register for the FortiGuard Analysis and Management Service. FortiGuard Analysis and Management Service is a subscription-based service and is purchased by contacting support.

After registering, you can back up or restore your configuration. FortiGuard Analysis and Management Service is useful when administering multiple FortiGate units without having a FortiManager unit. Using this service, you can also upgrade the firmware. Upgrading the firmware is available in the *Firmware Upgrade* section of the backup and restore menu.

When restoring the configuration from a remote location, a list of revisions is displayed so that you can choose the configuration file to restore.

The FortiGuard-FortiManager protocol is used when connecting to the FortiGuard Analysis and Management Service. This protocol runs over SSL using IPv4/TCP port 541 and includes the following functions:

- detects FortiGate unit dead or alive status
- detects management service dead or alive status
- notifies the FortiGate units about configuration changes, AV/IPS database update and firewall changes.

Restoring your firmware configuration

Administrators can restore a configuration file that was backed up using the *System Information* widget. If the configuration file was encrypted, you will need the password to restore the configuration file.

Local PC	Select to back up the configuration file to a local management computer.
FortiManager	Select to back up the configuration file to a FortiManager unit. The Central Management settings must be enabled and a FortiManager unit connected with the FortiGate unit so that the FortiGate unit can send the configuration file to the FortiManager unit. To enable central management, go to *System* > *Admin* > *Settings*.
USB Disk	Select to back up the configuration file to a USB key that is connected to the FortiGate unit.
Filename	Select Browse to locate the configuration file.
Password	If a password was set when saving the configuration file, enter the password.

Viewing online administrators

The *System Information* widget enables you to view information about the administrators logged into the FortiGate unit. To view logged in administrators, in the *System Information* widget, select *Details*.

Changing the currently logged in administrator's password

Use the *System Information* widget, to change your password. To do this, select the *Change Password* option in the *Current Administrator* row.

License Information widget

The *License Information* widget displays the status of your technical support contract and FortiGuard subscriptions. The FortiGate unit updates the license information status indicators automatically when attempting to connect to the FortiGuard Distribution Network (FDN). FortiGuard Subscriptions status indicators are green if the FDN was reachable and the license was valid during the last connection attempt, grey if the FortiGate unit cannot connect to the FDN, and orange if the FDN is reachable but the license has expired.

When a new FortiGate unit is powered on, it automatically searches for FortiGuard services. If the FortiGate unit is configured for central management, it will look for FortiGuard services on the configured FortiManager system. The FortiGate unit sends its serial number to the FortiGuard service provider, which then determines whether the FortiGate unit is registered and has valid contracts for FortiGuard subscriptions and FortiCare support services. If the FortiGate unit is registered and has a valid contract, the License Information is updated.

If the FortiGate unit is not registered, any administrator with the super_admin profile sees a reminder message that provides access to a registration form.

When a contract is due to expire within 30 days, any administrator with the super_admin profile sees a notification message that provides access to an Add Contract form. Simply enter the new contract number and select *Add*. Fortinet Support also sends contract expiry reminders.

You can optionally disable notification for registration or contract inquiry using the `config system global` command in the CLI. Selecting any of the *Configure* options will take you to the Maintenance page.

Support Contract	Displays details about your current Fortinet Support contract. • If *Not Registered* appears, select *Register* to register the FortiGate unit. • If *Expired* appears, select *Renew* for information on renewing your technical support contract. Contact your local reseller. • If *Registered* appears, the name of the support that registered this FortiGate unit is also displayed. The various types of contracts that you currently have and the expiry date for each type. • You can select *Login Now* to log into the Fortinet Support account that registered this FortiGate unit.
FortiGuard Services	Displays your current licenses for services from FortiGuard. Select *Renew* to update any of the licenses.
FortiCloud	Displays details about your current FortiCloud subscription. If the green *Activate* button appears, select it to either create a new account or add the FortiGate unit to an existing account. If you have already activated FortiCloud, the name of the *Account* will be listed. Select *Launch Portal* to view your FortiCloud account in a web browser. Information on the current *Type* and *Storage* is also listed. You can select *Upgrade* to change the type of your FortiCloud account.
FortiClient Software	Displays FortiClient license details and the number of *Register* and *Allowed* FortiClient users. You can select *Details* for more information about the current FortiClient users.
FortiToken Mobile	Displays the number of *Assigned* and *Allowed* FortiTokens.
SMS	Displays the number of *Sent* and *Allowed* SMS messages. You can select *Add Messages* to configure a new SMS message.
Virtual Domain	Displays the maximum number of virtual domains the FortiGate unit supports with the current license. For high-end models, you can select the *Purchase More* link to purchase a license key through Fortinet technical support to increase the maximum number of VDOMs.

FortiGate unit Operation widget

The *Unit Operation* widget is an illustrated version of the FortiGate unit's front panel that shows the status of the FortiGate unit's network interfaces. Interfaces appears green when connected. Hover the mouse pointer over an interface to view further details.

Icons around the front panel indicate when the FortiGate unit is connected to a FortiAnalyzer or FortiManager device, or FortiClient installations. Select the icon in the widget to jump to the configuration page for each device. When connected to one of these devices, a green check mark icon appears next to the icon. If the device communication is configured but the device is unreachable, a red X appears.

System Resources widget

The *System Resources* widget displays basic FortiGate unit resource usage. This widget displays the information for CPU and memory in either real-time or historical data. For FortiGate units with multiple CPUs, you can view the CPU usage as an average of all CPUs or each one individually.

This widget also is where you reboot or shutdown the FortiGate unit.

The options to reboot or shutdown the FortiGate unit are not available for an admin using the *prof_admin* profile.

Use the *Refresh* icon when you want to view current system resource information, regardless of whether you are viewing real-time or historical type format.

To change the resource view from real-time to historical, or change the CPU view (for multiple CPU FortiGate units), select the *Edit* icon (visible when you hover the mouse over the widget).

When viewing CPU and memory usage in the web-based manager, only the information for core processes displays. CPU for management processes, is excluded. For example, HTTPS connections to the web-based manager.

Alert Message Console widget

The *Alert Messages Console* widget helps you monitor system events on your FortiGate unit such as firmware changes, network security events, or virus detection events. Each message shows the date and time that the event occurred.

You can configure the alert message console settings to control what types of messages are displayed on the console.

To configure the Alert Message Console

1. Locate the *Alert Message Console* widget within the Dashboard menu.
2. Select the *Edit* icon in the *Alert Message Console* title bar.
3. Select the types of alerts that you do not want to be displayed in the widget.
4. Select *OK*.

CLI Console widget

The *CLI Console* widget enables you to access the CLI without exiting from the web-based manager.

The two controls located on the CLI Console widget title bar are *Customize*, and *Detach*.

- *Detach* moves the CLI Console widget into a pop-up window that you can resize and reposition. Select *Attach*. to move the widget back to the dashboard's page.
- *Customize* enables you to change the appearance of the console by selecting fonts and colors for the text and background.

Session History widget

The *Session History* widget displays the total session activity on the device. Activity displays on a per second basis. Select the *Edit* icon in the title bar (which appears when you hover the mouse over the widget) to change the time period for the widget.

Top Sessions widget

The *Top Sessions* widget polls the FortiGate unit for session information for IPv4 or IPv6 addresses, or both. Rebooting the FortiGate unit will reset the Top Session statistics to zero.

When you select *Details* to view the current sessions list, a list of all sessions currently processed by the FortiGate unit.

Detailed information is available in *System* > *Monitor* > *Sessions*. Use the following table to modify the default settings of the Top Sessions widget.

USB Modem widget

The *USB modem* widget enables you to monitor the status of your USB modem, and configure it as needed.

Advanced Threat Protection Statistics widget

The *Advanced Threat Protection Statistics* widget displays a count of detected malware and files scanned for these types of intrusions. It also displays statics on the number of files sent to FortiSandbox and the results from sandboxing.

Features widget

The *Features* widget displays a number of *Basic Features* and *Security Features* and whether or not each feature is currently enabled or disabled. Options for features that are disabled will not appear in the web-based manager.

For *Security Features*, several *Preset* options are available, which can be selected from the dropdown menu in the widget:

- *UTM* enabled all security features and should be chosen for networks that require full protection from FortiOS. *UTM* is the default setting.
- *WF* enables web filtering features.
- *ATP* enables protection against viruses and other external threats.
- *NGFW* enables application control and protection from external attacks.
- *NGFW* + *ATP* enables features that protect against external threats and attacks.

RAID monitor widget

The *RAID Monitor* widget displays the current state of the RAID array and each RAID disk. This widget does not display unless the FortiGate unit has more than one disk installed and is not available for FortiOS Carrier.

Array status icon	Displays the status of the RAID array. • Green with a check mark shows a healthy RAID array. • Yellow triangle shows the array is in a degraded state but it is still functioning. A degraded array is slower than a healthy array. Rebuild the array to fix the degraded state. • A wrench shows the array is being rebuilt. Positioning the mouse over the array status icon displays a text message of the status of the array.
Disk status icon	There is one icon for each disk in the array. • Green with a check mark shows a healthy disk. • Red with an X shows the disk has failed and needs attention. Positioning the mouse over the disk status icon displays the status of the disk, and the storage capacity of the disk.
RAID Level	The RAID level of this RAID array. The RAID level is set as part of configuring the RAID array.
Status bar	The bar shows the percentage of the RAID array that is currently in use.
Used/Free/Total	Displays the amount of RAID array storage that is being used, the amount of storage that is free, and the total storage in the RAID array. The values are in gigabytes.

RAID disk configuration

The RAID disk is configured from the Disk Configuration page.

RAID level	Select the level of RAID. Options include: • **RAID-0** — (striping) better performance, no redundancy • **RAID-1** — (mirroring) half the storage capacity, with redundancy • **RAID-5** — striping with parity checking, and redundancy Available RAID level options depend on the available number of hard disks. Two or more disks are required for RAID 0 or RAID 1. Three or more disks are required for RAID 5. Changing the RAID level will erase any stored log information on the array, and reboot the FortiGate unit. The FortiGate unit will remain offline while it reconfigures the RAID array. When it reboots, the array will need to synchronize before being fully operational.

Status	The status, or health, of RAID array. This status can be one of: • **OK** — standard status, everything is normal • **OK (Background-Synchronizing) (%)** — synchronizing the disks after changing RAID level, Synchronizing progress bar shows percent complete • **Degraded** — One or more of the disks in the array has failed, been removed, or is not working properly. A warning is displayed about the lack of redundancy in this state. Also, a degraded array is slower than a healthy array. Select *Rebuild RAID* to fix the array. • **Degraded (Background-Rebuilding) (%)** — The same as degraded, but the RAID array is being rebuilt in the background. The array continues to be in a fragile state until the rebuilding is completed.
Size	The size of the RAID array in gigabytes (GB). The size of the array depends on the RAID level selected, and the number of disks in the array.
Rebuild RAID	Select to rebuild the array after a new disk has been added to the array, or after a disk has been swapped in for a failed disk. If you try to rebuild a RAID array with too few disks you will get a rebuild error. After inserting a functioning disk, the rebuild will start. This button is only available when the RAID array is in a degraded state and has enough disks to be rebuilt. You cannot restart a rebuild once a rebuild is already in progress. **Note:** If a disk has failed, the number of working disks may not be enough for the RAID level to function. In this case, replace the failed disk with a working disk to rebuild the RAID array.
Disk#	The disk's position in the array. This corresponds to the physical slot of the disk. If a disk is removed from the FortiGate unit, the disk is marked as not a member of the array and its position is retained until a new disk is inserted in that drive bay.
Status	The status of this disk. Options include OK, and unavailable. A disk is unavailable if it is removed or has failed.

Basic configurations

Before going ahead and configuring security policies, users, and security profiles, you should perform some basic configurations to set up your FortiGate unit.

Changing your administrator password

By default, you can log in to the web-based manager by using the admin administrator account and no password. It is highly recommended that you add a password to the admin administrator account. For improved security, you should regularly change the admin administrator account password and the passwords for any other administrator accounts that you add.

To change an administrator's password, go to *System* > *Admin* > *Administrators*, edit the administrator account, and then change the password.

For details on selecting a password, and password best practices, see "Passwords" on page 57.

For information about resetting a lost administrator's password, see docs.fortinet.com/sysadmin.html.

Changing the web-based manager language

The default language of the web-based manager is English. To change the language, go to *System* > *Admin* > *Settings*. In the *Display Settings section*, select the language you want from the *Language* drop-down list.

For best results, you should select the language that the management computer operating system uses.

Changing administrative access

Through administrative access, an administrator can connect to the FortiGate unit. Access is available through a number of services, including HTTPS and SSH.The default configuration allows administrative access to one or more of the unit's interfaces as described in the *QuickStart Guide*.

To change administrative access

1. Go to *System* > *Network* > *Interface*.
2. Select the interface.
3. Select the administrative access type or types for that interface.
4. Select *OK*.

Changing the web-based manager idle timeout

By default, the web-based manager disconnects administrative sessions if no activity occurs for five minutes. This prevents someone from using the web-based manager if the management PC is left unattended.

To change the idle timeout

1. Go to *System* > *Admin* > *Settings*.
2. In the *Administration Settings* section, enter the time in minutes in the *Idle Timeout* field
3. Select *Apply*.

Switching VDOMs

When VDOMs are enabled, a menu appears in the left column called *Current VDOM*. This menu displays a drop-down list that lists the configured VDOMs.

To switch to a VDOM using the *Current VDOM* menu, select the VDOM that you want to switch to from the drop-down list. You are automatically redirected to that VDOM.

VDOMs are enabled on the *System Information* Dashboard Widget.

Connecting to the CLI from the web-based manager

You can use the CLI to configure all configuration options available from the web-based manager. Some configuration options are available only from the CLI.

To connect to the CLI console, go to *System* > *Dashboard* > *Status* and select inside the window of the *CLI Console* widget to automatically connect. For more information on using the CLI, see “Using the CLI” on page 33.

Logging out

Select the Logout icon to quit your administrative session. If you only close the browser or leave the web-based manager to surf to another web site, you remain logged in until the idle timeout (default 5 minutes) expires. To change the timeout, see “Changing the web-based manager idle timeout” on page 31.

Using the CLI

The command line interface (CLI) is an alternative configuration tool to the web-based manager. While the configuration of the web-based manager uses a point-and-click method, the CLI requires typing commands or uploading batches of commands from a text file, like a configuration script.

This section also explains common CLI tasks that an administrator does on a regular basis and includes the topics:

Connecting to the CLI

You can access the CLI in two ways:

- Locally — Connect your computer directly to the FortiGate unit's console port. Local access is required in some cases:
  - If you are installing your FortiGate unit for the first time and it is not yet configured to connect to your network, unless you reconfigure your computer's network settings for a peer connection, you may only be able to connect to the CLI using a local serial console connection. For more information, see "Connecting to the CLI" on page 55.
  - Restoring the firmware utilizes a boot interrupt. Network access to the CLI is not available until after the boot process has completed, making local CLI access the only viable option.
- Through the network — Connect your computer through any network attached to one of the FortiGate unit's network ports. The network interface must have enabled Telnet or SSH administrative access if you will connect using an SSH/Telnet client, or HTTP/HTTPS administrative access if you will connect using the *CLI Console* widget in the web-based manager.

Connecting to the CLI using a local console

Local console connections to the CLI are formed by directly connecting your management computer or console to the FortiGate unit, using its DB-9 or RJ-45 console port. To connect to the local console you need:

- a computer with an available serial communications (COM) port
- the RJ-45-to-DB-9 or null modem cable included in your FortiGate package
- terminal emulation software such as HyperTerminal for Microsoft Windows

The following procedure describes connection using Microsoft HyperTerminal software; steps may vary with other terminal emulators.

To connect to the CLI using a local serial console connection

1. Using the null modem or RJ-45-to-DB-9 cable, connect the FortiGate unit's console port to the serial communications (COM) port on your management computer.
2. On your management computer, start HyperTerminal.
3. For the *Connection Description*, enter a *Name* for the connection, and select *OK*.
4. On the *Connect using* drop-down list box, select the communications (COM) port on your management computer you are using to connect to the FortiGate unit.
5. Select *OK*.
6. Select the following *Port* settings and select *OK*.

Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

7. Press Enter or Return on your keyboard to connect to the CLI.
8. Type a valid administrator account name (such as `admin`) and press Enter.
9. Type the password for that administrator account and press Enter. (In its default state, there is no password for the `admin` account.)

   The CLI displays the following text:

   ```
   Welcome!

   Type ? to list available commands.
   ```

   You can now enter CLI commands, including configuring access to the CLI through SSH or Telnet. For details, see "Enabling access to the CLI through the network (SSH or Telnet)" on page 34.

Enabling access to the CLI through the network (SSH or Telnet)

SSH or Telnet access to the CLI is accomplished by connecting your computer to the FortiGate unit using one of its RJ-45 network ports. You can either connect directly, using a peer connection between the two, or through any intermediary network.

If you do not want to use an SSH/Telnet client and you have access to the web-based manager, you can alternatively access the CLI through the network using the *CLI Console* widget in the web-based manager.

You must enable SSH and/or Telnet on the network interface associated with that physical network port. If your computer is not connected directly or through a switch, you must also configure the FortiGate unit with a static route to a router that can forward packets from the FortiGate unit to your computer. You can do this using either a local console connection or the web-based manager.

Requirements

- a computer with an available serial communications (COM) port and RJ-45 port
- terminal emulation software such as HyperTerminal for Microsoft Windows
- the RJ-45-to-DB-9 or null modem cable included in your FortiGate package
- a network cable
- prior configuration of the operating mode, network interface, and static route (for details, see)

To enable SSH or Telnet access to the CLI using a local console connection

1. Using the network cable, connect the FortiGate unit's network port either directly to your computer's network port, or to a network through which your computer can reach the FortiGate unit.
2. Note the number of the physical network port.
3. Using a local console connection, connect and log into the CLI. For details, see "Connecting to the CLI using a local console" on page 33.
4. Enter the following command:

```
config system interface
  edit <interface_str>
    set allowaccess <protocols_list>
    next
end
```

   where:

   - `<interface_str>` is the name of the network interface associated with the physical network port and containing its number, such as `port1`
   - `<protocols_list>` is the complete, space-delimited list of permitted administrative access protocols, such as `https ssh telnet`

   For example, to exclude HTTP, HTTPS, SNMP, and PING, and allow only SSH and Telnet administrative access on `port1`:

```
set system interface port1 config allowaccess ssh telnet
```

5. To confirm the configuration, enter the command to display the network interface's settings.

```
get system interface <interface_str>
```

   The CLI displays the settings, including the allowed administrative access protocols, for the network interfaces.

   To connect to the CLI through the network interface, see "Connecting to the CLI using SSH" on page 35 or "Connecting to the CLI using Telnet" on page 36.

Connecting to the CLI using SSH

Once the FortiGate unit is configured to accept SSH connections, you can use an SSH client on your management computer to connect to the CLI.

Secure Shell (SSH) provides both secure authentication and secure communications to the CLI. FortiGate units support 3DES and Blowfish encryption algorithms for SSH.

Before you can connect to the CLI using SSH, you must first configure a network interface to accept SSH connections. For details, see "Enabling access to the CLI through the network (SSH or Telnet)" on page 34. The following procedure uses PuTTY. Steps may vary with other SSH clients.

To connect to the CLI using SSH

1. On your management computer, start an SSH client.
2. In *Host Name (or IP Address)*, enter the IP address of a network interface on which you have enabled SSH administrative access.
3. In *Port*, enter `22`.
4. For the *Connection type*, select *SSH*.
5. Select *Open*.

   The SSH client connects to the FortiGate unit.

   The SSH client may display a warning if this is the first time you are connecting to the FortiGate unit and its SSH key is not yet recognized by your SSH client, or if you have previously connected to the FortiGate unit but used a different IP address or SSH key. This is normal If your management computer is directly connected to the FortiGate unit with no network hosts between them.
6. Click *Yes* to verify the fingerprint and accept the FortiGate unit's SSH key. You will not be able to log in until you have accepted the key.
7. The CLI displays a login prompt.
8. Type a valid administrator account name (such as `admin`) and press Enter.
9. Type the password for this administrator account and press Enter.

   The FortiGate unit displays a command prompt (its host name followed by a `#`). You can now enter CLI commands.

If three incorrect login or password attempts occur in a row, you will be disconnected. If this occurs, wait one minute, then reconnect to attempt the login again.

Connecting to the CLI using Telnet

Once the FortiGate unit is configured to accept Telnet connections, you can use a Telnet client on your management computer to connect to the CLI.

Telnet is not a secure access method. SSH should be used to access the CLI from the Internet or any other untrusted network.

Before you can connect to the CLI using Telnet, you must first configure a network interface to accept SSH connections. For details, see "Enabling access to the CLI through the network (SSH or Telnet)" on page 34.

To connect to the CLI using Telnet

1. On your management computer, start a Telnet client.
2. Connect to a FortiGate network interface on which you have enabled Telnet.
3. Type a valid administrator account name (such as `admin`) and press Enter.

4. Type the password for this administrator account and press Enter.

   The FortiGate unit displays a command prompt (its host name followed by a `#`). You can now enter CLI commands.

If three incorrect login or password attempts occur in a row, you will be disconnected. If this occurs, wait one minute, then reconnect to attempt the login again.

Command syntax

When entering a command, the command line interface (CLI) requires that you use valid syntax and conform to expected input constraints. It will reject invalid commands.

Fortinet documentation uses the following conventions to describe valid command syntax

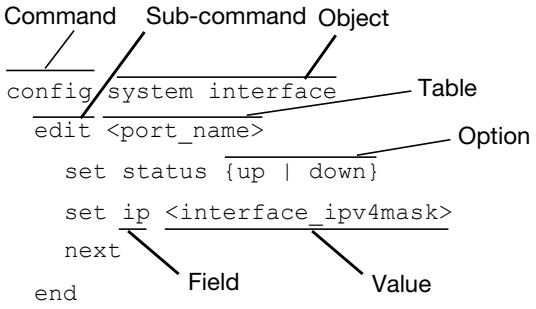
Terminology

Each command line consists of a command word that is usually followed by words for the configuration data or other specific item that the command uses or affects:

```
get system admin
```

To describe the function of each word in the command line, especially if that nature has changed between firmware versions, Fortinet uses terms with the following definitions.

Figure 2: Command syntax terminology



- **command** — A word that begins the command line and indicates an action that the FortiGate unit should perform on a part of the configuration or host on the network, such as `config` or `execute`. Together with other words, such as fields or values, that end when you press the Enter key, it forms a command line. Exceptions include multiline command lines, which can be entered using an escape sequence. (See “Shortcuts and key commands” on page 44.)

  Valid command lines must be unambiguous if abbreviated. (See “Command abbreviation” on page 45.) Optional words or other command line permutations are indicated by syntax notation. (See “Notation” on page 38.)
- **sub-command** — A kind of command that is available only when nested within the scope of another command. After entering a command, its applicable sub-commands are available to you until you exit the scope of the command, or until you descend an additional level into

another sub-command. Indentation is used to indicate levels of nested commands. (See "Indentation" on page 38.)

Not all top-level commands have sub-commands. Available sub-commands vary by their containing scope. (See "Sub-commands" on page 40.)

- **object** — A part of the configuration that contains tables and/or fields. Valid command lines must be specific enough to indicate an individual object.
- **table** — A set of fields that is one of possibly multiple similar sets which each have a name or number, such as an administrator account, policy, or network interface. These named or numbered sets are sometimes referenced by other parts of the configuration that use them. (See "Notation" on page 38.)
- **field** — The name of a setting, such as `ip` or `hostname`. Fields in some tables must be configured with values. Failure to configure a required field will result in an invalid object configuration error message, and the FortiGate unit will discard the invalid table.
- **value** — A number, letter, IP address, or other type of input that is usually your configuration setting held by a field. Some commands, however, require multiple input values which may not be named but are simply entered in sequential order in the same command line. Valid input types are indicated by constraint notation. (See "Notation" on page 38.)
- **option** — A kind of value that must be one or more words from of a fixed set of options. (See "Notation" on page 38.)

Indentation

Indentation indicates levels of nested commands, which indicate what other subcommittees are available from within the scope. For example, the `edit` sub-command is available only within a command that affects tables, and the `next` sub-command is available only from within the `edit` sub-command:

```
config system interface
   edit port1
      set status up
      next
end
```

For information about available sub-commands, see "Sub-commands" on page 40.

Notation

Brackets, braces, and pipes are used to denote valid permutations of the syntax. Constraint notations, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable value input.

Table 1: Command syntax notation

Convention	Description
Square brackets `[ ]`	A non-required word or series of words. For example: `[verbose {1 | 2 | 3}]` indicates that you may either omit or type both the `verbose` word and its accompanying option, such as `verbose 3`.

Table 1: Command syntax notation

Angle brackets < >	A word constrained by data type. The angled brackets contain a descriptive name followed by an underscore (_) and suffix that indicates the valid data type. For example, `<retries_int>`, indicates that you should enter a number of retries, such as `5`. Data types include: • `<xxx_name>`: A name referring to another part of the configuration, such as `policy_A`. • `<xxx_index>`: An index number referring to another part of the configuration, such as `0` for the first static route. • `<xxx_pattern>`: A regular expression or word with wild cards that matches possible variations, such as `*@example.com` to match all email addresses ending in `@example.com`. • `<xxx_fqdn>`: A fully qualified domain name (FQDN), such as `mail.example.com`. • `<xxx_email>`: An email address, such as `admin@example.com`. • `<xxx_ipv4>`: An IPv4 address, such as `192.168.1.99`. • `<xxx_v4mask>`: A dotted decimal IPv4 netmask, such as `255.255.255.0`. • `<xxx_ipv4mask>`: A dotted decimal IPv4 address and netmask separated by a space, such as `192.168.1.99 255.255.255.0`. • `<xxx_ipv4/mask>`: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as `192.168.1.1/24`. • `<xxx_ipv4range>`: A hyphen (`-`)-delimited inclusive range of IPv4 addresses, such as `192.168.1.1-192.168.1.255`. • `<xxx_ipv6>`: A colon(`:`)-delimited hexadecimal IPv6 address, such as `3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234`. • `<xxx_v6mask>`: An IPv6 netmask, such as `/96`. • `<xxx_ipv6mask>`: A dotted decimal IPv6 address and netmask separated by a space. • `<xxx_str>`: A string of characters that is not another data type, such as `P@ssw0rd`. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences. See “Special characters” on page 46. • `<xxx_int>`: An integer number that is ***not*** another data type, such as `15` for the number of minutes.
Curly braces `{ }`	A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets `[ ]`.

Table 1: Command syntax notation

Options delimited by vertical bars |	Mutually exclusive options. For example: `{enable | disable}` indicates that you must enter either `enable` or `disable`, but must not enter both.

Options delimited by spaces	Non-mutually exclusive options. For example:
	`{http https ping snmp ssh telnet}`
	indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as:
	`ping https ssh`

Sub-commands

Each command line consists of a command word that is usually followed by words for the configuration data or other specific item that the command uses or affects:

```
get system admin
```

Sub-commands are available from within the scope of some commands.When you enter a sub-command level, the command prompt changes to indicate the name of the current command scope. For example, after entering:

```
config system admin
```

the command prompt becomes:

```
(admin)#
```

Applicable sub-commands are available to you until you exit the scope of the command, or until you descend an additional level into another sub-command.

For example, the `edit` sub-command is available only within a command that affects tables; the `next` sub-command is available only from within the `edit` sub-command:

```
config system interface
   edit port1
      set status up
      next
   end
```

Sub-command scope is indicated by indentation. See “Indentation” on page 38.

Available sub-commands vary by command.From a command prompt within `config`, two types of sub-commands might become available:

- commands affecting fields
- commands affecting tables

Table 2: Commands for tables

clone <table>	Clone (or make a copy of) a table from the current object.
	For example, in `config firewall policy`, you could enter the following command to clone security policy 27 to create security policy 30:
	`clone 27 to 39`
	In `config antivirus profile`, you could enter the following command to clone an antivirus profile named `av_pro_1` to create a new antivirus profile named `av_pro_2`:
	`clone av_pro_1 to av_pro_2`
	`clone` may not be available for all tables.

delete <table>	Remove a table from the current object. For example, in `config system admin`, you could delete an administrator account named `newadmin` by typing `delete newadmin` and pressing Enter. This deletes `newadmin` and all its fields, such as `newadmin`'s `first-name` and `email-address`. `delete` is only available within objects containing tables.
edit <table>	Create or edit a table in the current object. For example, in `config system admin`: • edit the settings for the default `admin` administrator account by typing `edit admin`. • add a new administrator account with the name `newadmin` and edit `newadmin`'s settings by typing `edit newadmin`. `edit` is an interactive sub-command: further sub-commands are available from within `edit`. `edit` changes the prompt to reflect the table you are currently editing. `edit` is only available within objects containing tables. In objects such as security policies, `<table>` is a sequence number. To create a new entry without the risk of overwriting an existing one, enter `edit 0`. The CLI initially confirms the creation of entry 0, but assigns the next unused number after you finish editing and enter `end`.
end	Save the changes to the current object and exit the `config` command. This returns you to the top-level command prompt.
get	List the configuration of the current object or table. • In objects, `get` lists the table names (if present), or fields and their values. • In a table, `get` lists the fields and their values. For more information on `get` commands, see the *CLI Reference*.

Table 2: Commands for tables

purge	Remove all tables in the current object. For example, in `config forensic user`, you could type `get` to see the list of user names, then type `purge` and then `y` to confirm that you want to delete all users. `purge` is only available for objects containing tables. **Caution:** Back up the FortiGate unit before performing a `purge`. `purge` cannot be undone. To restore purged tables, the configuration must be restored from a backup. **Caution:** Do not purge `system interface` or `system admin` tables. `purge` does not provide default tables. This can result in being unable to connect or log in, requiring the FortiGate unit to be formatted and restored.
rename <table> to <table>	Rename a table. For example, in `config system admin`, you could rename `admin3` to `fwadmin` by typing `rename admin3 to fwadmin`. `rename` is only available within objects containing tables.
show	Display changes to the default configuration. Changes are listed in the form of configuration commands.

Example of table commands

From within the `system admin` object, you might enter:

```
edit admin_1
```

The CLI acknowledges the new table, and changes the command prompt to show that you are now within the `admin_1` table:

```
new entry 'admin_1' added
(admin_1)#
```

Table 3: Commands for fields

abort	Exit both the `edit` and/or `config` commands without saving the fields.
append	Add an option to an existing list.
end	Save the changes made to the current table or object fields, and exit the `config` command. (To exit without saving, use `abort` instead.)
get	List the configuration of the current object or table. • In objects, `get` lists the table names (if present), or fields and their values. • In a table, `get` lists the fields and their values.
move	Move an object within a list, when list order is important. For example, rearranging security policies within the policy list.

Table 3: Commands for fields

next	Save the changes you have made in the current table's fields, and exit the `edit` command to the object prompt. (To save and exit completely to the root prompt, use `end` instead.) `next` is useful when you want to create or edit several tables in the same object, without leaving and re-entering the `config` command each time. `next` is only available from a table prompt; it is not available from an object prompt.
select	Clear all options except for those specified. For example, if a group contains members A, B, C, and D and you remove all users except for B, use the command `select member B`.
set <field> <value>	Set a field's value. For example, in `config system admin`, after typing `edit admin`, you could type `set password newpass` to change the password of the `admin` administrator to `newpass`. **Note:** When using `set` to change a field containing a space-delimited list, type the whole new list. For example, `set <field> <new-value>` will replace the list with the `<new-value>` rather than appending `<new-value>` to the list.
show	Display changes to the default configuration. Changes are listed in the form of configuration commands.
unselect	Remove an option from an existing list.
unset <field>	Reset the table or object's fields to default values. For example, in `config system admin`, after typing `edit admin`, typing `unset password` resets the password of the `admin` administrator account to the default (in this case, no password).

Example of field commands

From within the `admin_1` table, you might enter:

```
set password my1stExamplePassword
```

to assign the value `my1stExamplePassword` to the `password` field. You might then enter the `next` command to save the changes and edit the next administrator's table.

Permissions

Depending on the account that you use to log in to the FortiGate unit, you may not have complete access to all CLI commands. Access profiles control which CLI commands an administrator account can access. Access profiles assign either read, write, or no access to each area of the FortiGate software. To view configurations, you must have read access. To make changes, you must have write access.

Unlike other administrator accounts, the administrator account named `admin` exists by default and cannot be deleted. The `admin` administrator account is similar to a root administrator account. This administrator account always has full permission to view and change all FortiGate configuration options, including viewing and changing ***all*** other administrator accounts. Its name and permissions cannot be changed. It is the only administrator account that can reset

another administrator's password without being required to enter that administrator's existing password.

Set a strong password for the admin administrator account, and change the password regularly. By default, this administrator account has no password. Failure to maintain the password of the admin administrator account could compromise the security of your FortiGate unit.

For complete access to all commands, you must log in with the administrator account named `admin`.

Tips

Basic features and characteristics of the CLI environment provide support and ease of use for many CLI tasks.

Help

To display brief help during command entry, press the question mark (?) key.

- Press the question mark (?) key at the command prompt to display a list of the commands available and a description of each command.
- Type a word or part of a word, then press the question mark (?) key to display a list of valid word completions or subsequent words, and to display a description of each.

Shortcuts and key commands

Table 4: Shortcuts and key commands

Action	Keys
List valid word completions or subsequent words. If multiple words could complete your entry, display all possible completions with helpful descriptions of each.	?
Complete the word with the next available match. Press the key multiple times to cycle through available matches.	Tab
Recall the previous command. Command memory is limited to the current session.	Up arrow, or Ctrl + P
Recall the next command.	Down arrow, or Ctrl + N
Move the cursor left or right within the command line.	Left or Right arrow
Move the cursor to the beginning of the command line.	Ctrl + A
Move the cursor to the end of the command line.	Ctrl + E

Table 4: Shortcuts and key commands

Move the cursor backwards one word.	Ctrl + B
Move the cursor forwards one word.	Ctrl + F
Delete the current character.	Ctrl + D
Abort current interactive commands, such as when entering multiple lines. If you are not currently within an interactive command such as `config` or `edit`, this closes the CLI connection.	Ctrl + C
Continue typing a command on the next line for a multi-line command. For each line that you want to continue, terminate it with a backslash (\ ). To complete the command line, terminate it by pressing the spacebar and then the Enter key, without an immediately preceding backslash.	\ then Enter

Command abbreviation

You can abbreviate words in the command line to their smallest number of non-ambiguous characters.

For example, the command `get system status` could be abbreviated to `g sy st`.

Adding and removing options from lists

When adding options to a list, such as a user group, using the `set` command will remove the previous configuration. For example. if you wish to add user D to a user group that already contains members A, B, and C, the command would need to be `set member A B C D`. If only `set member D` was used, then all former members would be removed from the group.

However, there are additional commands which can be used instead of `set` for changing options in a list.

Table 5: Additional commands for lists

append	Add an option to an existing list. For example, `append member` would add user D to a user group while all previous group members are retained
select	Clear all options except for those specified. For example, if a group contains members A, B, C, and D and you remove all users except for B, use the command `select member B`.
unselect	Remove an option from an existing list. For example, `unselect member A` would remove member A from a group will all previous group members are retained.

Environment variables

The CLI supports the following environment variables. Variable names are case-sensitive.

Table 6: Environment variables

$USERFROM	The management access type (`ssh`, `telnet`, `jsconsole` for the *CLI Console* widget in the web-based manager, and so on) and the IP address of the administrator that configured the item.
$USERNAME	The account name of the administrator that configured the item.
$SerialNum	The serial number of the FortiGate unit.

For example, the FortiGate unit's host name can be set to its serial number.

```
config system global
  set hostname $SerialNum
end
```

As another example, you could log in as `admin1`, then configure a restricted secondary administrator account for yourself named `admin2`, whose `first-name` is `admin1` to indicate that it is another of your accounts:

```
config system admin
  edit admin2
    set first-name $USERNAME
```

Special characters

The characters <, >, (,), #, ', and " are not permitted in most CLI fields. These characters are special characters, also known as reserved characters.

You may be able to enter special character as part of a string's value by using a special command, enclosing it in quotes, or preceding it with an escape sequence — in this case, a backslash (\ ) character.

In other cases, different keystrokes are required to input a special character. If you need to enter ? as part of config, you first need to input CTRL-V. If you enter the question mark (?) without first using CTRL-V, the question mark has a different meaning in CLI: it will show available command options in that section.

For example, if you enter ? without CTRL-V:

```
edit "*.xe
token line: Unmatched double quote.
```

If you enter ? with CTRL-V:

```
edit "*.xe?"
new entry '*.xe?' added
```

Table 7: Entering special characters

Character	Keys
?	Ctrl + V then ?
Tab	Ctrl + V then Tab

Table 7: Entering special characters

Space (to be interpreted as part of a string value, not to end the string)	Enclose the string in quotation marks: "Security Administrator". Enclose the string in single quotes: 'Security Administrator'. Precede the space with a backslash: Security\ Administrator.
' (to be interpreted as part of a string value, not to end the string)	\'
" (to be interpreted as part of a string value, not to end the string)	\"
\	\\

Using grep to filter get and show command output

In many cases, the `get` and `show` (and `diagnose`) commands may produce a large amount of output. If you are looking for specific information in a large get or show command output, you can use the grep command to filter the output to only display what you are looking for. The `grep` command is based on the standard UNIX grep, used for searching text output based on regular expressions.

Use the following command to display the MAC address of the FortiGate unit internal interface:

```
get hardware nic internal | grep Current_HWaddr
Current_HWaddr                  00:09:0f:cb:c2:75
```

Use the following command to display all TCP sessions in the session list and include the session list line number in the output

```
get system session list | grep -n tcp
```

Use the following command to display all lines in HTTP replacement message commands that contain `URL` (upper or lower case):

```
show system replacemsg http | grep -i url
```

There are three additional options that can be applied to grep:

```
-A <num> After
-B <num> Before
-C <num> Context
```

The option `-f` is also available to support Fortinet contextual output, in order to show the complete configuration. The following example shows the difference in output when `-f` option is used versus when it is not.

Using -f:

```
show | grep -f ldap-group1
   config user group
      edit "ldap-group1"
         set member "pc40-LDAP"
      next
   end
   config firewall policy
      edit 2
         set srcintf "port31"
         set dstintf "port32"
         set srcaddr "all"
         set action accept
         set identity-based enable
         set nat enable
         config identity-based-policy
            edit 1
               set schedule "always"
               set groups "ldap-group1"
               set dstaddr "all"
               set service "ALL"
            next
         end
      next
   end
```

Without using -f:

```
show | grep ldap-group1
   edit "ldap-group1"
      set groups "ldap-group1"
```

Language support and regular expressions

Characters such as ñ, é, symbols, and ideographs are sometimes acceptable input. Support varies by the nature of the item being configured. CLI commands, objects, field names, and options must use their exact ASCII characters, but some items with arbitrary names or values may be input using your language of choice. To use other languages in those cases, you must use the correct encoding.

Input is stored using Unicode UTF-8 encoding but is not normalized from other encodings into UTF-8 before it is stored. If your input method encodes some characters differently than in UTF-8, your configured items may not display or operate as expected.

Regular expressions are especially impacted. Matching uses the UTF-8 character values. If you enter a regular expression using another encoding, or if an HTTP client sends a request in an encoding other than UTF-8, matches may not be what you expect.

For example, with Shift-JIS, backslashes (\ ) could be inadvertently interpreted as the symbol for the Japanese yen (¥) and vice versa. A regular expression intended to match HTTP requests containing money values with a yen symbol therefore may not work it if the symbol is entered using the wrong encoding.

For best results, you should:

- use UTF-8 encoding, or
- use only the characters whose numerically encoded values are the same in UTF-8, such as the US-ASCII characters that are also encoded using the same values in ISO 8859-1, Windows code page 1252, Shift-JIS and other encodings, or
- for regular expressions that must match HTTP requests, use the same encoding as your HTTP clients.

HTTP clients may send requests in encodings other than UTF-8. Encodings usually vary by the client's operating system or input language. If you cannot predict the client's encoding, you may only be able to match any parts of the request that are in English, because regardless of the encoding, the values for English characters tend to be encoded identically. For example, English words may be legible regardless of interpreting a web page as either ISO 8859-1 or as GB2312, whereas simplified Chinese characters might only be legible if the page is interpreted as GB2312.

If you configure your FortiGate unit using other encodings, you may need to switch language settings on your management computer, including for your web browser or Telnet/SSH client. For instructions on how to configure your management computer's operating system language, locale, or input method, see its documentation.

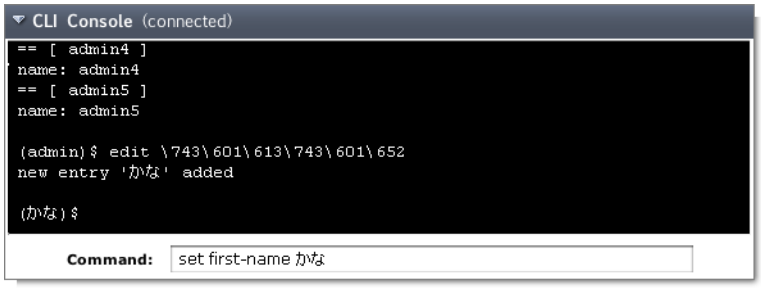
If you choose to configure parts of the FortiGate unit using non-ASCII characters, verify that all systems interacting with the FortiGate unit also support the same encodings. You should also use the same encoding throughout the configuration if possible in order to avoid needing to switch the language settings of the web-based manager and your web browser or Telnet/SSH client while you work.

Similarly to input, your web browser or CLI client should usually interpret display output as encoded using UTF-8. If it does not, your configured items may not display correctly in the web-based manager or CLI. Exceptions include items such as regular expressions that you may have configured using other encodings in order to match the encoding of HTTP requests that the FortiGate unit receives.

To enter non-ASCII characters in the CLI Console widget

1. On your management computer, start your web browser and go to the URL for the FortiGate unit's web-based manager.
2. Configure your web browser to interpret the page as UTF-8 encoded.
3. Log in to the FortiGate unit.
4. Go to *System* > *Dashboard* > *Status*.
5. In title bar of the *CLI Console* widget, click *Edit* (the pencil icon).
6. Enable *Use external command input box*.
7. Select *OK*.
8. The *Command* field appears below the usual input and display area of the *CLI Console* widget.
9. In *Command*, type a command.

Figure 3: Entering encoded characters *(CLI Console* widget)



10. Press Enter.

In the display area, the *CLI Console* widget displays your previous command interpreted into its character code equivalent, such as:

```
edit \743\601\613\743\601\652
```

and the command's output.

To enter non-ASCII characters in a Telnet/SSH client

1. On your management computer, start your Telnet or SSH client.
2. Configure your Telnet or SSH client to send and receive characters using UTF-8 encoding.

   Support for sending and receiving international characters varies by each Telnet/SSH client. Consult the documentation for your Telnet/SSH client.
3. Log in to the FortiGate unit.
4. At the command prompt, type your command and press Enter.

Figure 4: Entering encoded characters (PuTTY)

You may need to surround words that use encoded characters with single quotes (').

Depending on your Telnet/SSH client's support for your language's input methods and for sending international characters, you may need to interpret them into character codes before pressing Enter.

For example, you might need to enter:

```
edit '\743\601\613\743\601\652'
```

5. The CLI displays your previous command and its output.

Screen paging

You can configure the CLI to pause after displaying each page's worth of text when displaying multiple pages of output. When the display pauses, the last line displays `--More--`. You can then either:

- press the spacebar to display the next page.
- type `Q` to truncate the output and return to the command prompt.

This may be useful when displaying lengthy output, such as the list of possible matching commands for command completion, or a long list of settings. Rather than scrolling through or possibly exceeding the buffer of your terminal emulator, you can simply display one page at a time.

To configure the CLI display to pause when the screen is full:

```
config system console
  set output more
end
```

Baud rate

You can change the default baud rate of the local console connection.

To change the baud rate enter the following commands:

```
config system console
  set baudrate {115200 | 19200 | 38400 | 57600 | 9600}
end
```

Editing the configuration file on an external host

You can edit the FortiGate configuration on an external host by first backing up the configuration file to a TFTP server. Then edit the configuration file and restore it to the FortiGate unit.

Editing the configuration on an external host can be timesaving if you have many changes to make, especially if your plain text editor provides advanced features such as batch changes.

To edit the configuration on your computer

1. Use `execute backup` to download the configuration file to a TFTP server, such as your management computer.
2. Edit the configuration file using a plain text editor that supports Unix-style line endings.

Do not edit the first line. The first line(s) of the configuration file (preceded by a # character) contains information about the firmware version and FortiGate model. If you change the model number, the FortiGate unit will reject the configuration file when you attempt to restore it.

3. Use `execute restore` to upload the modified configuration file back to the FortiGate unit.

   The FortiGate unit downloads the configuration file and checks that the model information is correct. If it is, the FortiGate unit loads the configuration file and checks each command for errors. If a command is invalid, the FortiGate unit ignores the command. If the configuration file is valid, the FortiGate unit restarts and loads the new configuration.

Using Perl regular expressions

Some FortiGate features, such as spam filtering and web content filtering can use either wildcards or Perl regular expressions.

See http://perldoc.perl.org/perlretut.html for detailed information about using Perl regular expressions. For more information on using Perl expressions see the *Security Profiles* chapter of *The Handbook*.

Differences between regular expression and wildcard pattern matching

In Perl regular expressions, the period (‘.’) character refers to any single character. It is similar to the question mark (‘?’) character in wildcard pattern matching. As a result:

- `example.com` not only matches `example.com` but also matches `exampleacom`, `examplebcom`, `examplecom` and so on.

To match a special character such as the period ('.') and the asterisk (‘*’), regular expressions use the slash (‘\’) escape character. For example:

- To match `example.com`, the regular expression should be `example\.com`.

In Perl regular expressions, the asterisk (‘*’) means match 0 or more times of the character before it, not 0 or more times of any character. For example:

- `exam*\.com` matches `exammmm.com` but does not match `eample.com`.

To match any character 0 or more times, use ‘.*’ where ‘.’ means any character and the ‘*’ means 0 or more times. For example:

- the wildcard match pattern `exam*.com` is equivalent to the regular expression `exam.*\.com`.

Word boundary

In Perl regular expressions, the pattern does not have an implicit word boundary. For example, the regular expression “test” not only matches the word “test” but also matches any word that contains the word “test” such as “atest”, “mytest”, “testimony”, “atestb”. The notation “\b” specifies the word boundary. To match exactly the word “test”, the expression should be `\btest\b`.

Case sensitivity

Regular expression pattern matching is case sensitive in the Web and Spam filters. To make a word or phrase case insensitive, use the regular expression `/i`. For example, `/bad language/i` will block all instances of “bad language” regardless of case.

Table 8: Perl regular expression examples

Expression	Matches
abc	abc (that exact character sequence, but anywhere in the string)
^abc	abc at the beginning of the string
abc$	abc at the end of the string
a|b	either of a and b
^abc|abc$	the string abc at the beginning or at the end of the string
ab{2,4}c	an a followed by two, three or four b's followed by a c
ab{2,}c	an a followed by at least two b's followed by a c
ab*c	an a followed by any number (zero or more) of b's followed by a c
ab+c	an a followed by one or more b's followed by a c
ab?c	an a followed by an optional b followed by a c; that is, either abc or ac
a.c	an a followed by any single character (not newline) followed by a c

Table 8: Perl regular expression examples

a\.c	a.c exactly
[abc]	any one of a, b and c
[Aa]bc	either of Abc and abc
[abc]+	any (nonempty) string of a's, b's and c's (such as a, abba, acbabcacaa)
[^abc]+	any (nonempty) string which does not contain any of a, b and c (such as defg)
\d\d	any two decimal digits, such as 42; same as \d{2}
/i	makes the pattern case insensitive. For example, `/bad language/i` blocks any instance of “bad language” regardless of case.
\w+	a "word": a nonempty sequence of alphanumeric characters and low lines (underscores), such as foo and 12bar8 and foo_1
100\s*mk	the strings 100 and mk optionally separated by any amount of white space (spaces, tabs, newlines)
abc\b	abc when followed by a word boundary (e.g. in abc! but not in abcd)
perl\B	perl when not followed by a word boundary (e.g. in perlert but not in perl stuff)
\x	tells the regular expression parser to ignore white space that is neither backslashed nor within a character class. You can use this to break up your regular expression into (slightly) more readable parts.

Basic Administration

The FortiGate unit requires some basic configuration to add it to your network. These basic steps include assigning IP addresses, adding routing, and configuring security policies. Until the administrator completes these steps, inter-network and Internet traffic will not flow through the unit.

There are two methods of configuring the FortiGate unit: the web-based manager or the command line interface (CLI). This chapter will step through both methods to complete the basic configurations to put the device on your network. Use whichever you are most comfortable with.

This chapter also provides guidelines for password and administrator best practices as well as how to upgrade the firmware.

This section includes the topics:

- Connecting to the FortiGate unit
- System configuration
- Passwords
- Administrators
- Configuration backups
- Firmware
- Controlled upgrade

For setup and configuration of your specific FortiGate models, see the *QuickStart Guide* for that model.

Connecting to the FortiGate unit

To configure, maintain and administer the FortiGate unit, you need to connect to it from a management computer. There are two ways to do this:

- using the web-based manager: a GUI interface that you connect to using a current web browser, such as Firefox or Internet Explorer.
- using the command line interface (CLI): a command line interface similar to DOS or UNIX commands that you connect to using SSH or a Telnet terminal.

Connecting to the web-based manager

To connect to the web-based manager, you require:

- a computer with an Ethernet connection
- Microsoft Internet Explorer version 6.0 or higher or any recent version of a common web browser
- an Ethernet cable.

To connect to the web-based manager

1. Set the IP address of the management computer to the static IP address `192.168.1.2` with a netmask of `255.255.255.0`.
2. Using the Ethernet cable, connect the internal or port 1 interface of the FortiGate unit to the computer Ethernet connection.
3. Start your browser and enter the address `https://192.168.1.99`. (remember to include the “s” in `https://`).

   To support a secure HTTPS authentication method, the FortiGate unit ships with a self-signed security certificate that is offered to remote clients whenever they initiate a HTTPS connection to the FortiGate unit. When you connect, the FortiGate unit displays two security warnings in a browser.

   The first warning prompts you to accept and optionally install the FortiGate unit’s self-signed security certificate. If you do not accept the certificate, the FortiGate unit refuses the connection. If you accept the certificate, the FortiGate login page appears. The credentials entered are encrypted before they are sent to the FortiGate unit. If you choose to accept the certificate permanently, the warning is not displayed again.

   Just before the FortiGate login page is displayed, a second warning informs you that the FortiGate certificate distinguished name differs from the original request. This warning occurs because the FortiGate unit redirects the connection. This is an informational message. Select *OK* to continue logging in.
4. Type `admin` in the Name field and select Login.

Connecting to the CLI

The command line interface (CLI) is an alternative method of configuring the FortiGate unit. The CLI compliments the web-based manager in that it not only has the same configuration options, but also contains additional settings not available through the web-based manager.

If you are new to FortiOS or a command line interface configuration tool, see “Using the CLI” on page 33 for an overview of the CLI, how to connect to it, and how to use it.

System configuration

Once the FortiGate unit is connected and traffic can pass through, several more configuration options are available. While not mandatory, they will help to ensure better control with the firewall.

Setting the time and date

For effective scheduling and logging, the FortiGate system date and time should be accurate. You can either manually set the system date and time or configure the FortiGate unit to automatically keep its time correct by synchronizing with a Network Time Protocol (NTP) server.

To set the date and time - web-based manager

1. Go to *System* > *Dashboard* > *Status*.
2. Under *System Information* > *System Time*, select *Change*.
3. Select your *Time Zone*.
4. Select *Set Time* and set the FortiGate system date and time.
5. Select *OK*.

Set the time and date - CLI

```
config system global
  set timezone <zone_value>
end
execute date [<date_str>]
execute time [<time_str>]
```

By default, FortiOS has the daylight savings time configuration enabled. The system time must be manually adjusted after daylight saving time ends. To disable DST, enter the following command in the CLI:

```
config system global
  set dst disable
end
```

Using the NTP Server

The Network Time Protocol enables you to keep the FortiGate time in sync with other network systems. By enabling NTP on the FortiGate unit, FortiOS will check with the NTP server you select at the configured intervals. This will also ensure that logs and other time-sensitive settings on the FortiGate unit are correct.

The FortiGate unit maintains its internal clock using a built-in battery. At startup, the time reported by the FortiGate unit will indicate the hardware clock time, which may not be accurate. When using NTP, the system time might change after the FortiGate has successfully obtained the time from a configured NTP server.

For the NTP server, you can identify a specific port/IP address for this self-originating traffic. The configuration is performed in the CLI with the command set `source-ip`. For example, to set the source IP of NTP to be on the DMZ1 port with an IP of 192.168.4.5, the commands are:

```
config system ntp
  set ntpsyn enable
  set syncinterval 5
  set source-ip 192.168.4.5
end
```

Configuring FortiGuard

FortiGuard is Fortinet's threat research and response team. With more than 200 security engineers and forensic analysts around the globe providing 24 hours a day, 365 days a year analysis of current threats on the Internet, the FortiGuard team's sole purpose is to protect customers.

The FortiGuard Distribution Network (FDN) is a world-wide network of FortiGuard Distribution Servers (FDS). When the FortiGate unit connects to the FDN, it connects to the nearest FDS. To do this, all FortiGate units are programmed with a list of FDS addresses sorted by nearest time zone according to the time zone configured for the FortiGate unit.

Before you can begin receiving updates, you must register your FortiGate unit from the Fortinet webpage. After registering, you need to configure the FortiGate unit to connect to the FDN to update antivirus, antispam, and IPS attack definitions.

Updating antivirus and IPS definitions

After you have registered your FortiGate unit, you can update the definitions for antivirus and IPS. The FortiGuard Center enables you to receive push updates, allow push update to a specific IP address, and schedule updates for daily, weekly, or hourly intervals.

To update antivirus definitions and IPS signatures

1. Go to *System* > *Config* > *FortiGuard*.
2. Select the expand arrow for *AV and IPS Options*.
3. Select *Update Now* to update the antivirus definitions.

   If the connection to the FDN is successful, the web-based manager displays a message similar to the following:

Your update request has been sent. Your database will be updated in a few minutes. Please check your update page for the status of the update.

After a few minutes, if an update is available, the FortiGuard Center Services information on the Dashboard lists new version information for antivirus definitions. The System Status page also displays new dates and version numbers for the antivirus definitions. Messages are recorded to the event log indicating whether or not the update was successful or not.

Updating antivirus definitions can cause a very short disruption in traffic currently being scanned while the FortiGate unit applies the new signature database. Schedule updates when traffic is light, for example overnight, to minimize any disruption.

Passwords

The FortiGate unit ships with a default admin account that has no password. You will want to apply a password to prevent anyone from logging into the FortiGate unit and changing configuration options.

To change the administrator password - web-based manager

1. Go to *System* > *Admin* > *Administrators*.
2. Select the admin account and select *Change Password*.
3. Enter a new password and select *OK*.

Set the admin password - CLI

```
config system admin
  edit admin
    set password <admin_password>
end
```

Password considerations

When changing the password, consider the following to ensure better security.

- Do not make passwords that are obvious, such as the company name, administrator names, or other obvious word or phrase.
- Use numbers in place of letters, for example, `passw0rd`. Alternatively, spell words with extra letters, for example, *password*.
- Administrative passwords can be up to 64 characters.

- Include a mixture of letters, numbers, and upper and lower case.
- Use multiple words together, or possibly even a sentence, for example keytothehighway.
- Use a password generator.
- Change the password regularly and always make the new password unique and not a variation of the existing password, such as changing from `password` to `password1`.
- Write the password down and store it in a safe place away from the management computer, in case you forget it or ensure that at least two people know the password in the event that one person becomes ill, is away on vacation or leaves the company. Alternatively, have two different admin logins.

Password policy

The FortiGate unit includes the ability to enforce a password policy for administrator login. With this policy, you can enforce regular changes and specific criteria for a password including:

- minimum length between 8 and 64 characters.
- if the password must contain uppercase (A, B, C) and/or lowercase (a, b, c) characters.
- if the password must contain numbers (1, 2, 3).
- if the password must contain non-alphanumeric characters (!, @, #, $, %, ^, &, *, ().
- where the password applies (admin or IPsec or both).
- the duration of the password before a new one must be specified.

To apply a password policy - web-based manager

1. Go to *System* > *Admin* > *Settings*.
2. Select *Enable Password Policy* and configure the settings as required.

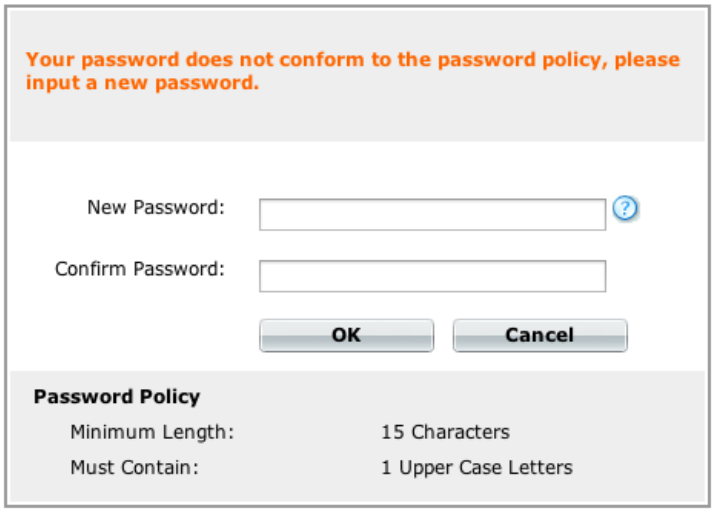
To apply a password policy - CLI

```
config system password-policy
  set status enable
```

Configure the other settings as required.

If you add a password policy or change the requirements on an existing policy, the next time that administrator logs into the FortiGate unit, they are prompted to update their password to meet the new requirements before proceeding to log in.

Figure 5: Password policy dialog box



Lost Passwords

If an administrator password has been lost, refer to the SysAdmin's Notebook article "Resetting a lost admin password," found at docs.fortinet.com/p/sysadmin-s-notebook-and-tech-notes.

Administrators

By default, the FortiGate unit has a super administrator called "admin". This user login cannot be deleted and always has ultimate access over the FortiGate unit. Additional administrators can be added for various functions, each with a unique username, password, and set of access privileges.

There are two levels of administrator accounts; regular administrators and system administrators. Regular administrators are administrators with any admin profile other than the default super_admin. System administrators are administrators that are assigned the super_admin profile, which has the highest level of access.

Adding administrators

The name of the administrator should not contain the characters <>()#"'. Using these characters in the administrator account name can result in a cross site scripting (XSS) vulnerability.

Only the default "admin" account or an administrator with read-write access control to add new administrator accounts and control their permission levels can create a new administrator account. If you log in with an administrator account that does not have the super_admin admin profile, the administrators list will show only the administrators for the current virtual domain.

When adding administrators, you are setting up the administrator's user account. An administrator account comprises of an administrator's basic settings as well as their access profile. The access profile is a definition of what the administrator is capable of viewing and editing.

To add an administrator - web-based manager

1. Go to *System* > *Admin* > *Administrators*.
2. Select *Create New*.
3. Enter the administrator name.
4. Select the type of account it will be. If you select *Remote*, the FortiGate unit can reference a RADIUS, LDAP or TACAS+ server.
5. When selecting *Remote* or *PKI* accounts, select the User Group the account will access.

   For information on logging in using remote authentication servers, see the *User Authentication Guide*. For an example of setting up a user with LDAP, see "LDAP Admin Access and Authorization" on page 60
6. Enter the password for the user.

   This may be a temporary password that the administrator can change later. Passwords can be up to 256 characters in length. For more information on passwords, see "Passwords" on page 57.
7. Select *OK*.

To add an administrator - CLI

```
config system admin
  edit <admin_name>
    set password <password>
    set accprofile <profile_name>
end
```

LDAP Admin Access and Authorization

You can use the LDAP server as a means to add administrative users, saving the time to add users to the FortiGate unit administrator list. After configuring, any user within the selected LDAP group server can automatically log into the FortiGate unit as an adm i st rat or. Ensure that the admin profile is the correct level of access, or the users within the LDAP group are the only ones authorized to configure or modify the configuration of the FortiGate unit.

To do this, requires three steps:

- configure the LDAP server
- add the LDAP server to a user group
- configure the administrator account

Configure the LDAP server

First set up the LDAP server as you normally would, and include a group to bind to.

To configure the LDAP server - web-based manager

1. Go to *User & Device* > *Remote* > *LDAP* and select *Create New*.
2. Enter a *Name* for the server.
3. Enter the *Server IP* address or name.
4. Enter the *Common Name Identifier* and *Distinguished Name*.
5. Set the *Bind Type to Regular* and enter the *User DN* and *Password*.
6. Select *OK*.

To configure the LDAP server - CLI

```
config user ldap
  edit <ldap_server_name>
    set server <server_ip>
    set cnid cn
    set dn DC=XYZ,DC=COM
    set type regular
    set username CN=Administrator,CN=Users,DC=XYZ,DC=COM
    set password <password>
    set member-attr <group_binding>
end
```

Add the LDAP server to a user group

Next, create a user group that will include the LDAP server that was created above.

To create a user group - web-based manager

1. Go to *User & Device* > *User Group* > *User Group* and select *Create New*.
2. Enter a *Name* for the group.

3. In the section labelled *Remote authentication servers*, select *Add*.
4. Select the *Remote Server* from the drop-down list.
5. Select *OK*.

To create a user group - CLI

```
config user group
  edit <group_name>
    config match
      edit 1
        set server-name <LDAP_server>
        set group-name <group_name>
    end
end
```

Configure the administrator account

Now you can create a new administrator, where rather than entering a password, you will use the new user group and the wildcard option for authentication.

To create an administrator - web-based manager

1. Go to *System* > *Admin* > *Administrators* and select *Create New*.
2. In the *Administrator* field, enter the name for the administrator.
3. For *Type*, select *Remote*.
4. Select the *User Group* created above from the drop-down list.
5. Select *Wildcard*.
6. The Wildcard option allows for LDAP users to connect as this administrator.
7. Select an *Admin Profile*.
8. Select *OK*.

To create an administrator - CLI

```
config system admin
  edit <admin_name>
    set remote-auth enable
    set accprofile super_admin
    set wildcard enable
    set remote-group ldap
end
```

Monitoring administrators

You can view the administrators logged in using the *System Information* widget on the Dashboard. On the widget is the *Current Administrator* row that shows the administrator logged in and the total logged in. Selecting *Details* displays the administrators), where they are logging in from and how (CLI, web-based manager) and when they logged in.

You are also able to monitor the activities the administrators perform on the FortiGate unit using the logging of events. Event logs include a number of options to track configuration changes.

To set logging - web-based manager

1. Go to *Log & Report* > *Log Config* > *Log Settings*.
2. Under *Event Logging*, ensure *System activity event* is selected.
3. Select *Apply*.

To set logging - CLI

```
config log eventfilter
   set event enable
   set system enable
end
```

To view the logs go to *Log & Report* > *Event Log*.

Administrator profiles

Administer profiles define what the administrator user can do when logged into the FortiGate unit. When you set up an administrator user account, you also assign an administrator profile, which dictates what the administrator user will see. Depending on the nature of the administrator's work, access level or seniority, you can allow them to view and configure as much, or as little, as required.

super_admin profile

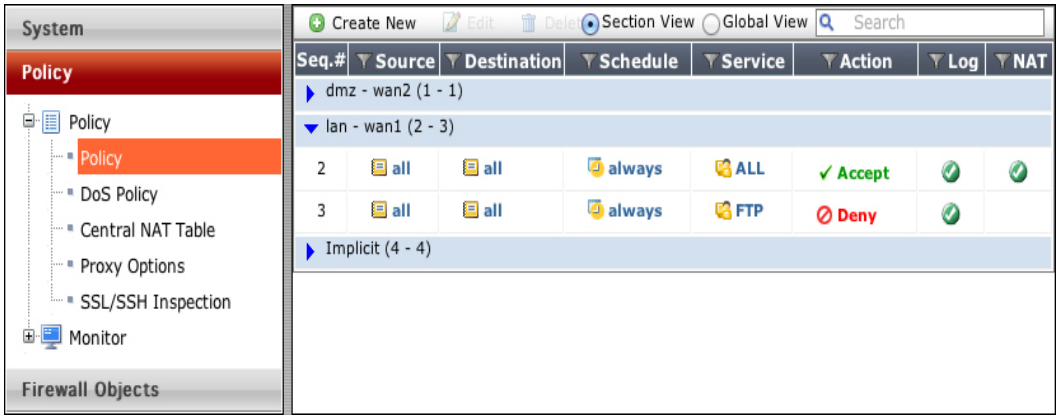
The super_admin administrator is the administrative account that the primary administrator should have to log into the FortiGate unit. The profile can not be deleted or modified to ensure there is always a method to administer the FortiGate unit.This user profile has access to all components of FortiOS, including the ability to add and remove other system administrators. For some administrative functions, such as backing up and restoring the configuration using SCP, super_admin access is required.

Creating profiles

To configure administrator profiles go to *System* > *Admin* > *Admin Profiles*. You can only assign one profile to an administrator user.

On the *New Admin Profile* page, you define the components of FortiOS that will be available to view and/or edit. For example, if you configure a profile so that the administrator can only access the firewall components, when an administrator with that profile logs into the FortiGate unit, they will only be able to view and edit any firewall components including policies, addresses, schedules and any other settings that directly affect security policies.

Figure 6: The view of an administrator with firewall-only access



Global and vdom profiles

By default, when you add a new administrative profile, it is set to have a vdom scope. That is, only the super_admin has a global profile that enables configuration of the entire FortiGate unit.

There may be instances where additional global administrative profiles may be required. To add more global profiles, use the following CLI command to set or change an administrative profile to be global.

```
config system accprofile
  set scope global
    ...
end
```

Once the scope is set, you can enable the read and read/write settings.

Regular (password) authentication for administrators

You can use a password stored on the local FortiGate unit to authenticate an administrator. When you select *Regular* for *Type*, you will see *Local* as the entry in the *Type* column when you view the list of administrators.

Management access

Management access defines how administrators are able to log on to the FortiGate unit to perform management tasks such as configuration and maintenance. Methods of access can include local access through the console connection or remote access over a network or modem interface using various protocols including Telnet and HTTPS.

You can configure management access on any interface in your VDOM. In NAT mode, the interface IP address is used for management access. In transparent mode, you configure a single management IP address that applies to all interfaces in your VDOM that permit management access. The FortiGate unit also uses this IP address to connect to the FDN for virus and attack updates.

The system administrator (admin) can access all VDOMs, and create regular administrator accounts. A regular administrator account can access only the VDOM to which it belongs and the management computer must connect to an interface in that VDOM. In both cases, the management computer must connect to an interface that permits management access and its IP address must be on the same network. Management access can be via HTTP, HTTPS, Telnet, or SSH sessions, if those services are enabled on the interface. HTTPS and SSH are preferred as they are more secure.

You can allow remote administration of the FortiGate unit. However, allowing remote administration from the Internet could compromise the security of the FortiGate unit. You should avoid this unless it is required for your configuration. The following precautions can be taken to improve the security of a FortiGate unit that allows remote administration from the Internet:

- Use secure administrative user passwords.
- Change these passwords regularly.
- Enable two-factor authentication for administrators.
- Enable secure administrative access to this interface using only HTTPS or SSH.
- Use Trusted Hosts to limit where the remote access can originate from.
- Do not change the system idle timeout from the default value of 5 minutes.

Security Precautions

One potential point of a security breach is at the management computer. Administrators who leave their workstations for a prolonged amount of time while staying logged into the web-based manager or CLI leave the firewall open to malicious intent.

Change the admin username and password

The default super administrator user name, admin, is a very standard, making it easy for someone with malicious intent to determine or guess. Having the correct user name is one half of the key to the FortiGate unit being compromised and so the default name should be changed.

To do this, you need to create another super user with full access and log in as that user. Then go to *System* > *Admin* > *Administrator,* select the *admin* account, and select *Edit* to change the user name.

If it has not been done already, the password should also be changed at this time. For tips about changing the password, see "Password considerations" on page 57.

Preventing unwanted login attempts

Setting trusted hosts for an administrator limits what computers an administrator can log in from, causing the FortiGate unit to only accept the administrator's login from the configured IP address. Any attempt to log in with the same credentials from any other IP address will be dropped.

Trusted hosts are configured when adding a new administrator by going to *System* > *Admin* > *Administrators* in the web-based manager or `config system admin` in the CLI.

To ensure the administrator has access from different locations, you can enter up to ten IP addresses, though ideally this should be kept to a minimum. For higher security, use an IP address with a net mask of 255.255.255.255, and enter an IP address (non-zero) in each of the three default trusted host fields. Also ensure all entries contain actual IP addresses, not the default 0.0.0.0.

The trusted hosts apply to the web-based manager, ping, snmp and the CLI when accessed through Telnet or SSH. CLI access through the console port is not affected.

Prevent multiple admin sessions

Multiple admin sessions can occur when multiple users access the FortiGate using the same admin account. By default, the FortiGate unit enables multiple logins of administrators using the same login credentials from different locations. To control admin log ins, and minimize the potential of configuration collisions, you can disable concurrent admin sessions. When disabled, only one user can use the admin account at a time. When a second admin attempts to connect, connection is denied with a message that the login attempt failed.

To disable concurrent admin sessions, enter the following command in the CLI:

```
config system global
  set admin-concurrent disable
end
```

On 2U FortiGate units, this option is also available in the Web-Based Manager by going to *System* > *Admin* > *Settings* and select *Allow each admin to log in with multiple sessions*.

Segregated administrative roles

To minimize the effect of an administrator causing errors to the FortiGate configuration and possibly jeopardizing the network, create individual administrative roles where none of the administrators have super-admin permissions. For example, one admin account is used solely to create security policies, another for users and groups, another for VPN, and so on.

Disable admin services

On untrusted networks, turn off the weak administrative services such as Telnet and HTTP. With these services, passwords are passed in the clear, not encrypted. These services can be disabled by going to *System* > *Network* > *Interface* and unselecting the required check boxes.

SSH login time out

When logging into the console using SSH, the default time of inactivity is 120 seconds (2 minutes) to successfully log into the FortiGate unit. To enhance security, you can configure the time to be shorter. Using the CLI, you can change the length of time the command prompt remains idle before the FortiGate unit will log the administrator out. The range can be between 10 and 3600 seconds.

To set the logout time enter the following commands:

```
config system global
  set admin-ssh-grace-time <number_of_seconds>
end
```

Administrator lockout

By default, the FortiGate unit includes set number of three password retries, allowing the administrator a maximum of three attempts to log into their account before they are locked out for a set amount of time (by default, 60 seconds).

The number of attempts can be set to an alternate value, as well as the default wait time before the administrator can try to enter a password again. You can also change this to further sway would-be hackers. Both settings are must be configured with the CLI

To configure the lockout options:

```
config system global
  set admin-lockout-threshold <failed_attempts>
  set admin-lockout-duration <seconds>
end
```

For example, to set the lockout threshold to one attempt and a five minute duration before the administrator can try again to log in enter the commands”

```
config system global
  set admin-lockout-threshold 1
  set admin-lockout-duration 300
end
```

Idle time-out

To avoid the possibility of an administrator walking away from the management computer and leaving it exposed to unauthorized personnel, you can add an idle time-out that will automatically log the user out if the web-based manager is not used for a specified amount of time. This will cause the administrator to log in to the device again in order to continue their work.

The time-out can be set as high as 480 minutes, or eight hours, although this is not recommend.

To set the idle time out - web-based manager

1. Go to *System* > *Admin* > *Settings*.
2. In the *Administration Settings*, enter the amount of time the Administrator login can remain idol in the *Idle Timeout* field.
3. Select *Apply*.

To set the idle time out - CLI

```
config system global
  set admintimeout <minutes>
end
```

Administrative ports

You can set the web-based manager access to use HTTP, HTTPS, SSH, and Telnet. In these cases, the default ports for these protocols are 80, 443, 22, and 23 respectively. You can change the ports used for network administration to a different, unused port to further limit potential hackers.

Ensure the port you select is not a port you will be using for other applications. For a list of assigned port numbers, see http://www.iana.org/assignments/port-numbers.

To change the administrative ports - web-based manager

1. Go to *System* > *Admin* > *Settings*.
2. In the *Web Administration Ports* section, change the port numbers.
3. Select *Apply.*

To change the administrative ports - CLI

```
config system global
  set admin-port <http_port_number>
  set admin-sport <https_port_number>
  set admin-ssh-port <ssh_port_number>
  set admin-telnet-port <telnet_port_number>
end
```

When logging into the FortiGate unit, by default FortiOS will automatically use the default ports. That is, when logging into the FortiGate IP address, you only need to enter the address, for example:

```
https://192.168.1.1
```

When you change the administrative port number, the port number must be added to the url. For example, if the port number for HTTPS access is 2112, the administrator must enter the following address:

```
https://192.168.1.1:2112
```

HTTPS redirect

When selecting port numbers for various protocols, you can also enable or disable the Redirect to HTTPS option. When enabled, if you select the Administrative Access for an interface to be

only HTTP, HTTPS will automatically be enabled, allowing the administrator access with either HTTP or HTTPS. The administrator can then log in using HTTPS for better security.

Note that if an SSL VPN is also configured for the same port, the SSL connection is over the HTTPS protocol. In these situations, the FortiGate unit will not redirect an HTTP address to the SSL VPN HTTPS address. Ideally, the administrator should not have the management address and an SSL VPN portal on the same interface.

Log in/out warning message

For administrators logging in and out of the FortiGate unit, you can include a login disclaimer. This disclaimer provides a statement that must be accepted or declined where corporations are governed by strict usage policies for forensics and legal reasons.

The disclaimer is enabled through the CLI.

To disable an interface:

```
config system global
  set pre-login-banner enable
  set post-login-banner enable
end
```

When set, once the administrator enters their user name and password, the disclaimer appears. They must select either Accept or Decline to proceed. When the post login is enabled, once the administrator logs out they are presented with the same message.

The banner is a default message that you can customize by going to *System* > *Config* > *Replacement Messages*. Select *Extended View* to see the *Admin* category and messages.

Disable the console interface

To prevent any unwanted login attempts using the COM communication port, you can disable login connections to the FortiGate unit.

This command is specifically for the COM port. You can still use FortiExplorer to connect and configure the FortiGate unit if required.

To disable an interface:

```
config system console
  set login disable
end
```

Disable interfaces

If any of the interfaces on the FortiGate unit are not being used, disable traffic on that interface. This avoids someone plugging in network cables and potentially causing network bypass or loop issues.

To disable an interface - web-based manager

1. Go to *System* > *Network* > *Interface*.
2. Select the interface from the list and select *Edit*.
3. For *Administrative Access*, select *Down*.
4. Select *OK*.

To disable an interface - CLI

```
config system interface
  edit <inerface_name>
    set status down
end
```

RADIUS authentication for administrators

Remote Authentication and Dial-in User Service (RADIUS) servers provide authentication, authorization, and accounting functions. FortiGate units use the authentication and authorization functions of the RADIUS server. To use the RADIUS server for authentication, you must configure the server before configuring the FortiGate users or user groups that will need it.

If you have configured RADIUS support and a user is required to authenticate using a RADIUS server, the FortiGate unit sends the user's credentials to the RADIUS server for authentication. If the RADIUS server can authenticate the user, the user is successfully authenticated with the FortiGate unit. If the RADIUS server cannot authenticate the user, the FortiGate unit refuses the connection.

If you want to use a RADIUS server to authenticate administrators in your VDOM, you must configure the authentication before you create the administrator accounts. To do this you need to:

- configure the FortiGate unit to access the RADIUS server
- create the RADIUS user group
- configure an administrator to authenticate with a RADIUS server.

Configuring LDAP authentication for administrators

Lightweight Directory Access Protocol (LDAP) is an Internet protocol used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, printers, etc.

If you have configured LDAP support and an administrator is required to authenticate using an LDAP server, the FortiGate unit contacts the LDAP server for authentication. If the LDAP server cannot authenticate the administrator, the FortiGate unit refuses the connection.

If you want to use an LDAP server to authenticate administrators in your VDOM, you must configure the authentication before you create the administrator accounts. To do this you need to:

- configure an LDAP server
- create an LDAP user group
- configure an administrator to authenticate with an LDAP server.

To view the LDAP server list, go to *User & Device* > *Remote* > *LDAP*.

For more information, see "LDAP Admin Access and Authorization" on page 60.

TACACS+ authentication for administrators

Terminal Access Controller Access-Control System (TACACS+) is a remote authentication protocol that provides access control for routers, network access servers, and other network computing devices via one or more centralized servers.

If you have configured TACACS+ support and an administrator is required to authenticate using a TACACS+ server, the FortiGate unit contacts the TACACS+ server for authentication. If the TACACS+ server cannot authenticate the administrator, the connection is refused by the FortiGate unit.

If you want to use an TACACS+ server to authenticate administrators in your VDOM, you must configure the authentication before you create the administrator accounts. To do this you need to:

- configure the FortiGate unit to access the TACACS+ server
- create a TACACS+ user group
- configure an administrator to authenticate with a TACACS+ server.

PKI certificate authentication for administrators

Public Key Infrastructure (PKI) authentication uses a certificate authentication library that takes a list of peers, peer groups, and user groups and returns authentication successful or denied notifications. Users only need a valid certificate for successful authentication; no username or password is necessary.

To use PKI authentication for an administrator, you must configure the authentication before you create the administrator accounts. To do this you need to:

- configure a PKI user
- create a PKI user group
- configure an administrator to authenticate with a PKI certificate.

General Settings

Go to *System* > *Admin* > *Settings* to configure basic settings for administrative access, password policies and displaying additional options in the web-based manager.

Administrative port settings

The Administrative Settings enable you to change the default port configurations for administrative connections to the FortiGate unit for added security. When connecting to the FortiGate unit when the port has changed, the port must be included, such as `https://<ip_address>:<port>`. For example, if you are connecting to the FortiGate unit using port 99, the url would be `https://192.168.1.99:99`.

If you make a change to the default port number for HTTP, HTTPS, Telnet, or SSH, ensure that the port number is unique.

Password policies

Password policies, available by going to *System* > *Admin* > *Settings*, enable you to create a password policy that any administrator or user who updates their password, must follow. Using the available options you can define the required length of the password, what it must contain (numbers, upper and lower case, and so on) and an expiry time frame.

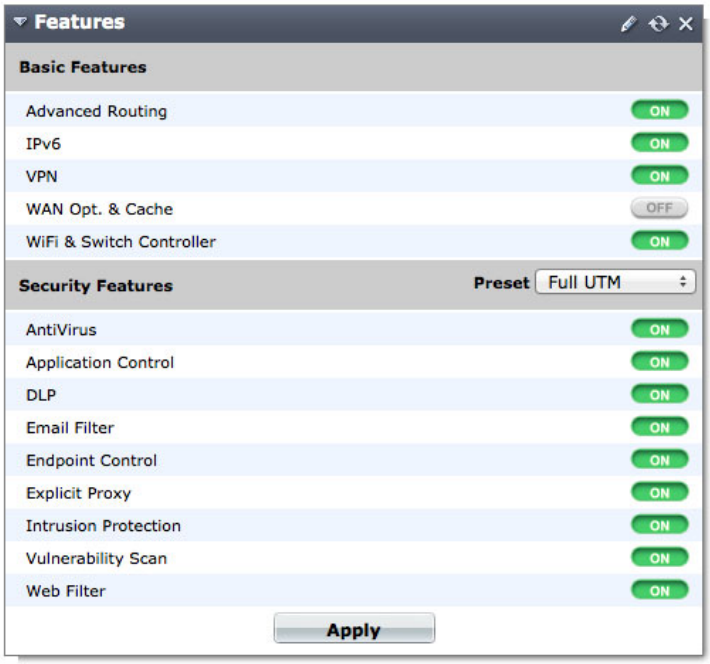
The FortiGate unit will warn of any password that is added and does not meet the criteria.

Feature Select

Feature Select is used to disable features which are not required for network administration. Disabling features also removes all related configuration options from the web-based manager.

Feature Select can be managed using the *Features* widget on the *Status* page. They can also be found at *System* > *Config* > *Features*, where additional features are also available by selecting *Show More*.

Figure 7: The Features widget



If a feature, such as IPv6, has been configured before being removed from the web-based manager, this configuration will still exist as part of the network, even though it is no longer visible using the web-based manager.

Configuration backups

Once you configure the FortiGate unit and it is working correctly, it is extremely important that you backup the configuration. In some cases, you may need to reset the FortiGate unit to factory defaults or perform a TFTP upload of the firmware, which will erase the existing configuration. In these instances, the configuration on the device will have to be recreated, unless a backup can be used to restore it.

It is also recommended that once *any* further changes are made that you backup the configuration immediately, to ensure you have the most current configuration available. Also, ensure you backup the configuration before upgrading the FortiGate unit's firmware. Should anything happen during the upgrade that changes the configuration, you can easily restore the saved configuration.

Always backup the configuration and store it on the management computer or off-site. You have the option to save the configuration file to various locations including the local PC, USB key, FTP and TFTP site.The latter two are configurable through the CLI only.

If you have VDOMs, you can back up the configuration of the entire FortiGate unit or only a specific VDOM. Note that if you are using FortiManager or FortiCloud, full backups are performed and the option to backup individual VDOMs will not appear.

To back up the FortiGate configuration - web-based manager

1. Go to *System* > *Dashboard* > *Status*.
2. On the *System Information* widget, select *Backup* for the *System Configuration*.

3. Select to backup to your *Local PC* or to a *USB key*.

   The *USB Disk* option will be grayed out if no USB drive is inserted in the USB port. You can also backup to the FortiManager using the CLI.
4. If VDOMs are enabled, select to backup the entire FortiGate configuration (*Full Config*) or only a specific VDOM configuration (*VDOM Config*).
5. If backing up a VDOM configuration, select the VDOM name from the list.
6. Select *Encrypt configuration file*.

   Encryption must be enabled on the backup file to back up VPN certificates.
7. Enter a password and enter it again to confirm it. You will need this password to restore the file.
8. Select *Backup*.
9. The web browser will prompt you for a location to save the configuration file. The configuration file will have a .conf extension.

To back up the FortiGate configuration - CLI

```
execute backup config management-station <comment>
```

… or …

```
execute backup config usb <backup_filename> [<backup_password>]
```

… or for FTP, note that port number, username are optional depending on the FTP site…

```
execute backup config ftp <backup_filename> <ftp_server> [<port>]
     [<user_name>] [<password>]
```

… or for TFTP …

```
execute backup config tftp <backup_filename> <tftp_servers>
     <password>
```

Use the same commands to backup a VDOM configuration by first entering the commands:

```
config vdom
  edit <vdom_name>
```

Backup and restore a configuration file using SCP

You can use secure copy protocol (SCP) to download the configuration file from the FortiGate unit as an alternative method of backing up the configuration file or an individual VDOM configuration file. This is done by enabling SCP for and administrator account and enabling SSH on a port used by the SCP client application to connect to the FortiGate unit. SCP is enabled using the CLI commands:

```
config system global
     set admin-scp enable
end
```

Use the same commands to backup a VDOM configuration by first entering the commands:

```
config global
  set admin-scp enable
end
config vdom
  edit <vdom_name>
```

Enable SSH access on the interface

SCP uses the SSH protocol to provide secure file transfer. The interface you use for administration must allow SSH access.

To enable SSH - web-based manager:

1. Go to *System* > *Network* > *Interface*.
2. Select the interface you use for administrative access and select *Edit*.
3. In the *Administrative Access* section, select *SSH*.
4. Select *OK*.

To enable SSH - CLI:

```
config system interface
    edit <interface_name>
        set allowaccess ping https ssh
  end
```

When adding to, or removing a protocol, you must type the entire list again. For example, if you have an access list of HTTPS and SSH, and you want to add PING, typing:

```
set allowaccess ping
```

...only PING will be set. In this case, you must type...

```
set allowaccess https ssh ping
```

Using the SCP client

The FortiGate unit downloads the configuration file as `sys_conf`. Use the following syntax to download the file:

Linux

```
scp admin@<FortiGate_IP>:fgt-config <location>
```

Windows

```
pscp admin@<FortiGate_IP>:fgt-config <location>
```

The following examples show how to download the configuration file from a FortiGate-100D, at IP address 172.20.120.171, using Linux and Windows SCP clients.

Linux client example

To download the configuration file to a local directory called `~/config`, enter the following command:

```
scp admin@172.20.120.171:fgt-config ~/config
```

Enter the admin password when prompted.

Windows client example

To download the configuration file to a local directory called c:\config, enter the following command in a Command Prompt window:

```
pscp admin@172.20.120.171:fgt-config c:\config
```

Enter the admin password when prompted.

SCP public-private key authentication

SCP authenticates itself to the FortiGate unit in the same way as an administrator using SSH accesses the CLI. Instead of using a password, you can configure the SCP client and the FortiGate unit with a public-private key pair.

To configure public-private key authentication

1. Create a public-private key pair using a key generator compatible with your SCP client.
2. Save the private key to the location on your computer where your SSH keys are stored.

   This step depends on your SCP client. The Secure Shell key generator automatically stores the private key.
3. Copy the public key to the FortiGate unit using the CLI commands:

```
config system admin
    edit admin
        set ssh-public-key1 "<key-type> <key-value>"
    end
```

   `<key-type>` must be the ssh-dss for a DSA key or ssh-rsa for an RSA key. For the `<key-value>`, copy the public key data and paste it into the CLI command.

   If you are copying the key data from Windows Notepad, copy one line at a time and ensure that you paste each line of key data at the end of the previously pasted data. As well:

   - Do not copy the end-of-line characters that appear as small rectangles in Notepad.
   - Do not copy the `---- BEGIN SSH2 PUBLIC KEY ---- or Comment: "[2048-bit dsa,...]"` lines.
   - Do not copy the `---- END SSH2 PUBLIC KEY ----` line.

4 Type the closing quotation mark and press Enter.

Your SCP client can now authenticate to the FortiGate unit based on SSH keys rather than the administrator password.

Restoring a configuration using SCP

To restore the configuration using SCP, use the commands:

```
scp <local_file> <admin_user>@<FGT_IP>:fgt_restore_config
```

To use this command/method of restoring the FortiGate configuration, you need to log in as the “admin” administrator.

Restoring a configuration

Should you need to restore a configuration file, use the following steps:

To restore the FortiGate configuration - web-based manager

1. Go to *System* > *Dashboard* > *Status*.
2. On the *System Information* widget, select *Restore* for the *System Configuration*.
3. Select to upload the configuration file to be restored from your *Local PC or a USB key*.

   The *USB Disk* option will be grayed out if no USB drive is inserted in the USB port. You can restore from the FortiManager using the CLI.
4. Enter the path and file name of the configuration file, or select *Browse* to locate the file.
5. Enter a password if required.
6. Select *Restore*.

To back up the FortiGate configuration - CLI

```
execute restore config management-station normal 0
```

… or …

```
execute restore config usb <filename> [<password>]
```

… or for FTP, note that port number, username are optional depending on the FTP site…

```
execute backup config ftp <backup_filename> <ftp_server> [<port>]
     [<user_name>] [<password>]
```

… or for TFTP …

```
execute backup config tftp <backup_filename> <tftp_server> <password>
```

The FortiGate unit will load the configuration file and restart. Once the restart has completed, verify that the configuration has been restored.

Configuration revisions

The *Revisions* options on the *System Information* widget enables you to manage multiple versions of configuration files. Revision control requires either a configured central management server, or FortiGate units with 512 MB or more of memory. The central management server can either be a FortiManager unit or the FortiCloud.

When revision control is enabled on your unit, and configurations have been backed up, a list of saved revisions of those backed-up configurations appears.

Restore factory defaults

There may be a point where need to reset the FortiGate unit to its original defaults; for example, to begin with a fresh configuration. There are two options when restoring factory defaults. The first resets the entire device to the original out-of-the-box configuration:

To reset the FortiGate unit to its factory default settings - web-based manager

1. Go to *System* > *Dashboard* > *Status*.
2. In the *System Information* widget, select *Restore* for the *System Configuration*.
3. Select *Restore Factory Defaults* at the top of the page.

You can reset using the CLI by entering the command:

```
execute factoryreset
```

When prompted, type `y` to confirm the reset.

Alternatively, in the CLI you can reset the factory defaults but retain the interface and VDOM configuration.

Use the command:

```
execute factoryreset2
```

Firmware

Fortinet periodically updates the FortiGate firmware to include new features and resolve important issues. After you have registered your FortiGate unit, you can download firmware updates from the support web site, http://support.fortinet.com.

The FortiGate unit includes a number of firmware installation options that enables you to test new firmware without disrupting the existing installation, and load it from different locations as required.

Before you install any new firmware, be sure to follow the steps below:

- review the *Release Notes* for a new firmware release.
- review the *Supported Upgrade Paths* document to make sure the upgrade from your current image to the desired new image is supported.
- backup the current configuration.
- download the new firmware image.
- test the patch release until you are satisfied that it applies to your configuration.

Installing a patch release without reviewing release notes or testing the firmware may result in changes to settings or unexpected issues.

Only FortiGate admin user and administrators whose access profiles contain system read and write privileges can change the FortiGate firmware.

Downloading firmware

Firmware images for all FortiGate units is available on the Fortinet Customer Support website. You must register your FortiGate unit to access firmware images. Register the FortiGate unit by visiting http://support.fortinet.com and select Product Registration.

To download firmware

1. Log into the site using your user name and password.
2. Go to *Firmware Images* > *FortiGate*.
3. Select the most recent FortiOS version.
4. Locate the firmware for your FortiGate unit, right-click the link and select the Download option for your browser.

Testing new firmware before installing

FortiOS enables you to test a new firmware image by installing the firmware image from a system reboot and saving it to system memory. After completing this procedure, the FortiGate unit operates using the new firmware image with the current configuration. This new firmware image is not permanently installed. The next time the FortiGate unit restarts, it operates with the originally installed firmware image using the current configuration. If the new firmware image operates successfully, you can install it permanently using the procedure "Upgrading the firmware - web-based manager" on page 77.

To use this procedure, you must connect to the CLI using the FortiGate console port and a RJ-45 to DB-9 or null modem cable. This procedure temporarily installs a new firmware image using your current configuration.

For this procedure you install a TFTP server that you can connect to from the FortiGate internal interface. The TFTP server should be on the same subnet as the internal interface.

To test the new firmware image

1. Connect to the CLI using a RJ-45 to DB-9 or null modem cable.
2. Make sure the TFTP server is running.
3. Copy the new firmware image file to the root directory of the TFTP server.
4. Make sure the FortiGate unit can connect to the TFTP server using the `execute ping` command.

5. Enter the following command to restart the FortiGate unit:

   ```
   execute reboot
   ```

6. As the FortiGate unit reboots, press any key to interrupt the system startup. As the FortiGate unit starts, a series of system startup messages appears.
   When the following messages appears:

   ```
   Press any key to display configuration menu....
   ```

7. Immediately press any key to interrupt the system startup.

You have only 3 seconds to press any key. If you do not press a key soon enough, the FortiGate unit reboots and you must login and repeat the execute reboot command.

If you successfully interrupt the startup process, the following messages appears:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B[: Boot with backup firmware and set as default
[C]: Configuration and information
[Q]: Quit menu and continue to boot with default
firmware.
[H]: Display this list of options.


Enter G, F, Q, or H:
```

8. Type G to get the new firmware image from the TFTP server.

   The following message appears:

   ```
   Enter TFTP server address [192.168.1.168]:
   ```

9. Type the address of the TFTP server and press Enter:

   The following message appears:

   ```
   Enter Local Address [192.168.1.188]:
   ```

10. Type an IP address of the FortiGate unit to connect to the TFTP server.

    The IP address must be on the same network as the TFTP server.

Make sure you do not enter the IP address of another device on this network.

The following message appears:

```
Enter File Name [image.out]:
```

11. Enter the firmware image file name and press Enter.

    The TFTP server uploads the firmware image file to the FortiGate unit and the following appears.

    ```
    Save as Default firmware/Backup firmware/Run image without saving:
        [D/B/R]
    ```

12. Type `R`.

    The FortiGate image is installed to system memory and the FortiGate unit starts running the new firmware image, but with its current configuration.

You can test the new firmware image as required. When done testing, you can reboot the FortiGate unit, and the FortiGate unit will resume using the firmware that was running before you installed the test firmware.

Upgrading the firmware - web-based manager

Installing firmware replaces your current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date.

Always remember to back up your configuration before making any changes to the firmware.

To upgrade the firmware

1. Log into the web-based manager as the admin administrative user.
2. Go to *System* > *Dashboard* > *Status*.
3. Under *System Information* > *Firmware Version*, select *Update*.
4. Type the path and filename of the firmware image file, or select *Browse* and locate the file.
5. Select *OK*.

   The FortiGate unit uploads the firmware image file, upgrades to the new firmware version, restarts, and displays the FortiGate login. This process takes a few minutes.

Upgrading the firmware - CLI

Installing firmware replaces your current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date. You can also use the CLI command `execute update-now` to update the antivirus and attack definitions. For more information, see the *FortiGate Administration Guide*.

Before you begin, ensure you have a TFTP server running and accessible to the FortiGate unit.

Always remember to back up your configuration before making any changes to the firmware.

To upgrade the firmware using the CLI

1. Make sure the TFTP server is running.
2. Copy the new firmware image file to the root directory of the TFTP server.
3. Log into the CLI.
4. Make sure the FortiGate unit can connect to the TFTP server.

   You can use the following command to ping the computer running the TFTP server. For example, if the IP address of the TFTP server is 192.168.1.168:

   ```
   execute ping 192.168.1.168
   ```

5. Enter the following command to copy the firmware image from the TFTP server to the FortiGate unit:

   ```
   execute restore image tftp <filename> <tftp_ipv4>
   ```

   Where `<name_str>` is the name of the firmware image file and `<tftp_ip4>` is the IP address of the TFTP server. For example, if the firmware image file name is `image.out` and the IP address of the TFTP server is 192.168.1.168, enter:

   ```
   execute restore image tftp image.out 192.168.1.168
   ```

   The FortiGate unit responds with the message:

```
This operation will replace the current firmware version!
     Do you want to continue? (y/n)
```

6. Type `y`.
7. The FortiGate unit uploads the firmware image file, upgrades to the new firmware version, and restarts. This process takes a few minutes.
8. Reconnect to the CLI.
9. Update antivirus and attack definitions, by entering:

   ```
   execute update-now
   ```

Installing firmware from a system reboot using the CLI

There is a possibility that the firmware upgrade does not load properly and the FortiGate unit will not boot, or continuously reboots. If this occurs, it is best to perform a fresh install of the firmware from a reboot using the CLI.

This procedure installs a firmware image and resets the FortiGate unit to default settings. You can use this procedure to upgrade to a new firmware version, revert to an older firmware version, or re-install the current firmware.

To use this procedure, you must connect to the CLI using the FortiGate console port and a RJ-45 to DB-9, or null modem cable. This procedure reverts the FortiGate unit to its factory default configuration.

For this procedure you install a TFTP server that you can connect to from the FortiGate internal interface. The TFTP server should be on the same subnet as the internal interface.

Before beginning this procedure, ensure you back up the FortiGate unit configuration.

If you are reverting to a previous FortiOS version, you might not be able to restore the previous configuration from the backup configuration file.

Installing firmware replaces your current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date.

To install firmware from a system reboot

1. Connect to the CLI using the RJ-45 to DB-9 or null modem cable.
2. Make sure the TFTP server is running.
3. Copy the new firmware image file to the root directory of the TFTP server.
4. Make sure the internal interface is connected to the same network as the TFTP server.
5. To confirm the FortiGate unit can connect to the TFTP server, use the following command to ping the computer running the TFTP server. For example, if the IP address of the TFTP server is 192.168.1.168:

   ```
   execute ping 192.168.1.168
   ```

6. Enter the following command to restart the FortiGate unit.

   ```
   execute reboot
   ```

   The FortiGate unit responds with the following message:

   ```
   This operation will reboot the system!
   Do you want to continue? (y/n)
   ```

7 Type `y`.

   As the FortiGate unit starts, a series of system startup messages appears. When the following messages appears:

   ```
   Press any key to display configuration menu.....
   ```

Immediately press any key to interrupt the system startup.

You have only 3 seconds to press any key. If you do not press a key soon enough, the FortiGate unit reboots and you must log in and repeat the execute reboot command.

If you successfully interrupt the startup process, the following messages appears:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B[: Boot with backup firmware and set as default
[C]: Configuration and information
[Q]: Quit menu and continue to boot with default
firmware.
[H]: Display this list of options.


Enter G, F, Q, or H:
```

8. Type G to get to the new firmware image form the TFTP server.

   The following message appears:

   ```
   Enter TFTP server address [192.168.1.168]:
   ```

9. Type the address of the TFTP server and press Enter:

   The following message appears:

   ```
   Enter Local Address [192.168.1.188]:
   ```

10. Type an IP address the FortiGate unit can use to connect to the TFTP server. The IP address can be any IP address that is valid for the network the interface is connected to.

Make sure you do not enter the IP address of another device on this network.

The following message appears:

```
Enter File Name [image.out]:
```

11. Enter the firmware image filename and press Enter.

    The TFTP server uploads the firmware image file to the FortiGate unit and a message similar to the following appears:

    ```
    Save as Default firmware/Backup firmware/Run image without saving:
         [D/B/R]
    ```

12 Type `D`.

The FortiGate unit installs the new firmware image and restarts. The installation might take a few minutes to complete.

Reverting to a previous firmware version - web-based manager

The following procedures revert the FortiGate unit to its factory default configuration and deletes any configuration settings.

If you are reverting to a previous FortiOS version, you might not be able to restore the previous configuration from the backup configuration file.

Always remember to back up your configuration before making any changes to the firmware.

To revert to a previous firmware version

1. Copy the firmware image file to the management computer.
2. Log into the FortiGate web-based manager.
3. Go to *System* > *Dashboard* > *Status*.
4. Under *System Information* > *Firmware Version*, select *Update*.
5. Type the path and filename of the firmware image file, or select Browse and locate the file.
6. Select *OK*.

   The FortiGate unit uploads the firmware image file, reverts to the old firmware version, resets the configuration, restarts, and displays the FortiGate login. This process takes a few minutes.
7. Log into the web-based manager.
8. Restore your configuration.

   For information about restoring your configuration see “Restoring a configuration” on page 73.

Reverting to a previous firmware version - CLI

This procedure reverts the FortiGate unit to its factory default configuration and deletes IPS custom signatures, web content lists, email filtering lists, and changes to replacement messages.

Before beginning this procedure, it is recommended that you:

- back up the FortiGate unit system configuration using the command `execute backup config`
- back up the IPS custom signatures using the command `execute backup ipsuserdefsig`
- back up web content and email filtering lists

To use the following procedure, you must have a TFTP server the FortiGate unit can connect to.

To revert to a previous firmware version using the CLI

1. Make sure the TFTP server is running
2. Copy the firmware image file to the root directory of the TFTP server.
3. Log into the FortiGate CLI.

4. Make sure the FortiGate unit can connect to the TFTP server execute by using the `execute ping` command.
5. Enter the following command to copy the firmware image from the TFTP server to the FortiGate unit:

   ```
   execute restore image tftp <name_str> <tftp_ipv4>
   ```

   Where `<name_str>` is the name of the firmware image file and `<tftp_ip4>` is the IP address of the TFTP server. For example, if the firmware image file name is `imagev28.out` and the IP address of the TFTP server is 192.168.1.168, enter:

   ```
   execute restore image tftp image28.out 192.168.1.168
   ```

   The FortiGate unit responds with this message:

```
This operation will replace the current firmware version!
     Do you want to continue? (y/n)
```

6. Type `y`.

   The FortiGate unit uploads the firmware image file. After the file uploads, a message similar to the following appears:

   ```
   Get image from tftp server OK.
        Check image OK.
        This operation will downgrade the current firmware version!
        Do you want to continue? (y/n)
   ```

7. Type `y`.
8. The FortiGate unit reverts to the old firmware version, resets the configuration to factory defaults, and restarts. This process takes a few minutes.
9. Reconnect to the CLI.
10. To restore your previous configuration, if needed, use the command:

    ```
    execute restore config <name_str> <tftp_ip4>
    ```

11. Update antivirus and attack definitions using the command:

    ```
    execute update-now.
    ```

Configuration Revision

The *Configuration Revisions* menu enables you to manage multiple versions of configuration files on models that have a 512 flash memory and higher. Revision control requires either a configured central management server or the local hard drive. The central management server can either be a FortiManager unit or FortiCloud.

If central management is not configured on your FortiGate unit, a message appears to tell you to do one of the following:

- enable central management (see Central management)
- obtain a valid license.

When revision control is enabled on your FortiGate unit, and configurations backups have been made, a list of saved revisions of those backed-up configurations appears.

Configuration revisions are viewed in the *System Information* widget on the Dashboard.

Backup and Restore from a USB key

Use a USB key to either backup a configuration file or restore a configuration file. You should always make sure a USB key is properly install before proceeding since the FortiGate unit must recognize that the key is installed in its USB port.

You can only save VPN certificates if you encrypt the file. Make sure the configuration encryption is enabled so you can save the VPN certificates with the configuration file. An encrypted file is ineffective if selected for the USB Auto-Install feature.

To backup configuration using the CLI

1. Log into the CLI.
2. Enter the following command to backup the configuration files:
   ```
   exec backup config usb <filename>
   ```
3. Enter the following command to check the configuration files are on the key:
   ```
   exec usb-disk list
   ```

To restore configuration using the CLI

1. Log into the CLI.
2. Enter the following command to restore the configuration files:
   ```
   exec restore image usb <filename>
   ```
   The FortiGate unit responds with the following message:
   ```
   This operation will replace the current firmware version!
   Do you want to continue? (y/n)
   ```
3. Type `y`.
4.

Backup and Restore an encrypted config file from a USB key

You can save and boot an encrypted configuration file from a USB key. The configuration will only load when rebooting the FortiGate unit with the USB key inserted.

The administrator must back up the configuration to the USB key using the command:

```
execute backup config usb-mode <password>
```

administrator backup the configuration, to the USB key ("exec backup config usb-mode")

Insert the USB key into any FortiGate unit running the same image/patch release as the FortiGate unit that created the configuration file

The Administrator runs the CLI command below to reboot the FortiGate unit and load the configuration file from the USB key:

```
execute restore config usb-mode <password>)
```

The FortiGate unit saves the password into the flash memory. When system boots, the FortiGate unit loads the configurations from the USB key using the saved password in the flash. This configuration is read-only. That is, no configuration changes can be made while running with the configuration. The administrator is not permitted to make any configuration changes while configurations are loaded from USB (read-only)

If the USB key is removed while the FortiGate unit is running, the FortiGate unit deletes the password from the flash memory and reboots.

Controlled upgrade

Using a controlled upgrade, you can upload a new version of the FortiOS firmware to a separate partition in the FortiGate memory for later upgrade. The FortiGate unit can also be configured so that when it is rebooted, it will automatically load the new firmware (CLI only). Using this option, you can stage a number of FortiGate units to do an upgrade simultaneously to all devices using FortiManager or script.

To load the firmware for later installation - web-based manager

1. Go to *System* > *Dashboard* > *Status*.
2. Under *System Information* > *Firmware Version*, select *Update*.
3. Type the path and filename of the firmware image file, or select *Browse* and locate the file.
4. Deselect the *Boot the New Firmware* option
5. Select *OK*.

To load the firmware for later installation - CLI

```
execute restore secondary-image {ftp | tftp | usb}
```

To set the FortiGate unit so that when it reboots, the new firmware is loaded, use the CLI command...

```
execute set-next-reboot {primary | secondary}
```

... where `{primary | secondary}` is the partition with the preloaded firmware.

To trigger the upgrade using the web-based manager

1. Go to *System* > *Dashboard* > *Status*.
2. Under *System Information* > *Firmware Version*, select *Details.*
3. Select the check box for the new firmware version.

   The *Comments* column indicates which firmware version is the current active version.
4. Select *Upgrade* icon.

Best practices

The FortiGate unit is installed, and traffic is moving. With your network sufficiently protected, you can now fine-tune the firewall for the best performance and efficiency. This chapter describes configuration options that can ensure your FortiGate unit is running at its best performance.

This section includes the topics on:

Hardware

Environmental specifications

Keep the following environmental specifications in mind when installing and setting up your FortiGate unit.

- Operating temperature: 32 to 104°F (0 to 40°C) (temperatures may vary, depending on the FortiGate model)
- If you install the FortiGate unit in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient temperature. Therefore, make sure to install the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature.
- Storage temperature: -13 to 158°F (-25 to 70°C) (temperatures may vary, depending on the FortiGate model)
- Humidity: 5 to 90% non-condensing
- Air flow - For rack installation, make sure that the amount of air flow required for safe operation of the equipment is not compromised.
- For free-standing installation, make sure that the appliance has at least 1.5 in. (3.75 cm) of clearance on each side to allow for adequate air flow and cooling.

This device complies with part FCC Class A, Part 15, UL/CUL, C Tick, CE and VCCI. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with

the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

The equipment compliance with FCC radiation exposure limit set forth for uncontrolled Environment.

Risk of Explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

To reduce the risk of fire, use only No. 26 AWG or larger UL Listed or CSA Certified Telecommunication Line Cord

Grounding

- Ensure the FortiGate unit is connected and properly grounded to a lightning and surge protector. WAN or LAN connections that enter the premises from outside the building should be connected to an Ethernet CAT5 (10/100 Mb/s) surge protector.
- Shielded Twisted Pair (STP) Ethernet cables should be used whenever possible rather than Unshielded Twisted Pair (UTP).
- Do not connect or disconnect cables during lightning activity to avoid damage to the FortiGate unit or personal injury.

Rack mount instructions

Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.

Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained.

Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

Shutting down

Always shut down the FortiGate operating system properly before turning off the power switch to avoid potential hardware problems.

To power off the FortiGate unit - web-based manager

1. Go to *System* > *Status*.
2. In the *System Resources* widget, select *Shutdown*.

To power off the FortiGate unit - CLI

```
execute shutdown
```

Once this has been done, you can safely turn off the power switch or disconnect the power cables from the power supply.

Performance

- Disable any management features you do not need. If you don't need SSH or SNMP, disable them. SSH also provides another possibility for would-be hackers to infiltrate your FortiGate unit.
- Put the most used firewall rules to the top of the interface list.
- Log only necessary traffic. The writing of logs, especially if to an internal hard disk, slows down performance.
- Enable only the required application inspections.
- Keep alert systems to a minimum. If you send logs to a syslog server, you may not need SNMP or email alerts, making for redundant processing.
- Establish scheduled FortiGuard updates at a reasonable rate. Daily updates occurring every 4-5 hours are sufficient for most situations. In more heavy-traffic situations, schedule updates for the evening when more bandwidth can be available.
- Keep security profiles to a minimum. If you do not need a profile on a firewall rule, do not include it.
- Keep VDOMs to a minimum. On low-end FortiGate units, avoid using them if possible.
- Avoid traffic shaping if you need maximum performance. Traffic shaping, by definition, slows down traffic.

Firewall

- Avoid using the *All* selection for the source and destination addresses. Use addresses or address groups.
- Avoid using *Any* for the services.
- Use logging on a policy only when necessary and be aware of the performance impact. For example, you may want to log all dropped connections but can choose to use this sparingly

by sampling traffic data rather than have it continually storing log information you may not use.

- Use the comment field to input management data, for example: who requested the rule, who authorized it, etc.
- Avoid FQDN addresses if possible, unless they are internal. It can cause a performance impact on DNS queries and security impact from DNS spoofing.
- If possible, avoid port ranges on services for security reasons.
- Use groups whenever possible.
- To ensure that all AV push updates occur, ensure you have an AV profile enabled in a security policy.

Intrusion protection

- Create and use security profiles with specific signatures and anomalies you need per-interface and per-rule.
- Do not use predefined or generic profiles. While these profiles are convenient to supply immediate protection, you should create profiles to suit your network environment.
- If you do use the default profiles, reduce the IPS signatures/anomalies enabled in the profile to conserve processing time and memory.
- If you are going to enable anomalies, make sure you tune thresholds according to your environment.
- If you need protection, but not audit information, disable the logging option.
- Tune the IP-protocol parameter accordingly.

Antivirus

- Enable only the protocols you need to scan. If you have antivirus scans occurring on the SMTP server, or use FortiMail, it is redundant to have scanning occur on the FortiGate unit as well.
- Reduce the maximum file size to be scanned. Viruses usually travel in small files of around 1 to 2 megabytes.
- Antivirus scanning within an HA cluster can impact performance.
- Enable grayware scanning on security profiles tied to Internet browsing.
- Do not quarantine files unless you regularly monitor and review them. This is otherwise a waste of space and impacts performance.
- Use file patterns to avoid scanning where it is not required.
- Enable heuristics from the CLI if high security is required using the command `config antivirus heuristic`.

Web filtering

- Web filtering within an HA cluster impacts performance.
- Always review the DNS settings to ensure the servers are fast.
- Content blocking may cause performance overhead.
- Local URL filters are faster than FortiGuard web filters, because the filter list is local and the FortiGate unit does not need to go out to the Internet to get the information from a FortiGuard web server.

Antispam

- If possible use, a FortiMail unit. The antispam engines are more robust.
- Use fast DNS servers.
- Use specific security profiles for the rule that will use antispam.
- DNS checks may cause false positive with HELO DNS lookup.
- Content analysis (banned words) may impose performance overhead.

Security

- Use NTP to synchronize time on the FortiGate and the core network systems, such as email servers, web servers, and logging services.
- Enable log rules to match corporate policy. For example, log administration authentication events and access to systems from untrusted interfaces.
- Minimize adhoc changes to live systems, if possible, to minimize interruptions to the network. When not possible, create backup configurations and implement sound audit systems using FortiAnalyzer and FortiManager.
- If you only need to allow access to a system on a specific port, limit the access by creating the strictest rule possible.

FortiGuard

The FortiGuard Distribution Network (FDN) of servers provides updates to antivirus, antispam and IPS definitions to your FortiGate unit. Worldwide coverage of FortiGuard services is provided by FortiGuard service points. FortiGuard Subscription Services provide comprehensive Unified Threat Management (UTM) security solutions to enable protection against content and network level threats.

The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGate units. The Global Threat Research Team enables Fortinet to deliver a combination of multi-layered security intelligence and provide true zero-day protection from new and emerging threats.The FortiGuard Network has data centers around the world located in secure, high availability locations that automatically deliver updates to the Fortinet security platforms to and protect the network with the most up-to-date information.

To ensure optimal response and updates, the FortiGate unit will contact a FortiGuard service point closest to the FortiGate installation, using the configured time zone information. FortiGuard services are continuously updated year-round, 24x7.

Every FortiGate unit includes a free 30-day FortiGuard trial license. FortiGuard license management is performed by Fortinet servers. The FortiGate unit automatically contacts a FortiGuard service point when enabling FortiGuard services. Contact Fortinet Technical Support to renew a FortiGuard license after the free trial.

This section includes the topics:

FortiGuard Services

The FortiGuard services provide a number of services to monitor world-wide activity and provide the best possible security.

Next Generation Firewall

The Next Generation Firewall (NGFW) offers integrated, high-performance protection against today's wide range of advanced threats targeting your applications, data, and users.

NGFW services include:

- ***Intrusion Prevention System (IPS)***- The FortiGuard Intrusion Prevention System (IPS) uses a customizable database of more than 4000 known threats to stop attacks that evade conventional firewall defenses. It also provides behavior-based heuristics, enabling the

system to recognize threats when no signature has yet been developed. It also provides more than 1000 application identity signatures for complete application control.

- ***Application Control*** - Application Control allows you to identify and control applications on networks and endpoints regardless of port, protocol, and IP address used. It gives you unmatched visibility and control over application traffic, even traffic from unknown applications and sources.

Advanced Threat Protection

Advanced Threat Protect (ATP) provides protection against a variety of threats, including Advanced Targeted Attacks (ATA), also known as Advanced Persistent Threats (APT).

ATP services include:

- ***Antivirus*** -The FortiGuard Antivirus Service provides fully automated updates to ensure protection against the latest content level threats. It employs advanced virus, spyware, and heuristic detection engines to prevent both new and evolving threats from gaining access to your network and protects against vulnerabilities.
- ***Web Filtering*** - Web Filtering provides Web URL filtering to block access to harmful, inappropriate, and dangerous web sites that may contain phishing/pharming attacks, malware such as spyware, or objectionable content that can expose your organization to legal liability. Based on automatic research tools and targeted research analysis, real-time updates enable you to apply highly-granular policies that filter web access based on 78 web content categories, over 45 million rated web sites, and more than two billion web pages - all continuously updated.

Other Services

FortiGuard provides a number of additional services, including:

- ***Vulnerability Scanning*** - FortiGuard Services provide comprehensive and continuous updates for vulnerabilities, remediation, patch scan, and configuration benchmarks.
- ***Email Filtering*** - The FortiGuard Antispam Service uses both a sender IP reputation database and a spam signature database, along with sophisticated spam filtering tools on Fortinet appliances and agents, to detect and block a wide range of spam messages. Updates to the IP reputation and spam signature databases are provided continuously via the FDN.
- ***Messaging Services*** - Messaging Services allow a secure email server to be automatically enabled on your FortiGate unit to send alert email or send email authentication tokens. With the SMS gateway, you can enter phone numbers where the FortiGate unit will send the SMS messages.

  Note that depending on your carrier, there may be a slight time delay on receiving messages.
- ***DNS and DDNS*** - The FortiGuard DNS and DDNS services provide an efficient method of DNS lookups once subscribed to the FortiGuard network. This is the default option. The FortiGate unit connects automatically to the FortiGuard DNS server. If you do not register, you need to configure an alternate DNS server.

  Configure the DDNS server settings using the CLI commands:

```
config system fortiguard
  set ddns-server-ip
  set ddns-server-port
end
```

Support Contract and FortiGuard Subscription Services

The *Support Contract* and *FortiGuard Subscription Services* sections are displayed in abbreviated form within the *License Information* widget. A detailed version is available by going to *System* > *Config* > *FortiGuard*.

The Support Contract area displays the availability or status of your FortiGate unit's support contract. The status displays can be either *Unreachable, Not Registered,* or *Valid Contract*.

The FortiGuard Subscription Services area displays detailed information about your FortiGate unit's support contract and FortiGuard subscription services. On this page, you can also manually update the antivirus and IPS engines.

The status icons for each section Indicates the state of the subscription service. The icon corresponds to the availability description.

- **Gray (Unreachable)** – the FortiGate unit is not able to connect to service.
- **Orange (Not Registered)** – the FortiGate unit can connect, but not subscribed.
- **Yellow (Expired)** – the FortiGate unit had a valid license that has expired.
- **Green (Valid license)** – the FortiGate unit can connect to FDN and has a registered support contract. If the Status icon is green, the expiry date also appears.

FortiCloud

FortiCloud is a hosted security management and log retention service for FortiGate products. It gives you a centralized reporting, traffic analysis, configuration and log retention without the need for additional hardware and software.

A subscription to FortiCloud also includes Cloud Sandbox, a service in which suspicious files can be inspected in isolation from your network.

For more information about FortiCloud, see "FortiCloud" on page 102.

Antivirus and IPS

The FortiGuard network is an always updating service, including grayware and signatures for application control. There are two methods of updating the virus and IPS signatures on your FortiGate unit: manually or through push updates.

Detection during update

During an update, the FortiGate unit will continue to detect to scan network traffic. Sessions occurring right before an update will be scanned using the current signatures. Sessions that occur during the update, when the signature database is reloading, will be on hold until the signatures load, at which point the new signatures are used to scan these sessions. Sessions occur i ng right after the update will also use the new signatures.

Antivirus and IPS Options

Go to *System* > *Config* > *FortiGuard*, and expand the *AV and IPS Options* section to configure the antivirus and IPS options for connecting and downloading definition files.

Use override server address	Select to configure an override server if you cannot connect to the FDN or if your organization provides updates using their own FortiGuard server.
Allow Push Update	Select to allow updates sent automatically to your FortiGate unit when they are available
Allow Push Update status icon	The status of the FortiGate unit for receiving push updates: • **Gray (Unreachable)** - the FortiGate unit is not able to connect to push update service • **Yellow (Not Available)** - the push update service is not available with your current support license • **Green (Available)** - the push update service is allowed.
Use override push IP and Port	Available only if both *Use override server address* and *Allow Push Update* are enabled. Enter the IP address and port of the NAT device in front of your FortiGate unit. FDS will connect to this device when attempting to reach the FortiGate unit. The NAT device must be configured to forward the FDS traffic to the FortiGate unit on UDP port 9443.
Schedule Updates	Select this check box to enable updates to be sent to your FortiGate unit at a specific time. For example, to minimize traffic lag times, you can schedule the update to occur on weekends or after work hours. Note that a schedule of once a week means any urgent updates will not be pushed until the scheduled time. However, if there is an urgent update required, select the *Update Now* button.
Update Now	Select to manually initiate an FDN update.
Submit attack characteristics… (recommended)	Select to help Fortinet maintain and improve IPS signatures. The information sent to the FortiGuard servers when an attack occurs and can be used to keep the database current as variants of attacks evolve.

Manual updates

To manually update the signature definitions file, you need to first go to the Support web site at https://support.fortinet.com. Once logged in, select FortiGuard Service Updates from the Download area of the web page. The browser will present you the most current antivirus and IPS signature definitions which you can download.

Once downloaded to your computer, log into the FortiGate unit to load the definition file.

To load the definition file onto the FortiGate unit

1. Go to *System* > *Config* > *FortiGuard*.
2. Select the *Update* link for either *AV Definitions or IPS Definitions*.
3. Locate the downloaded file and select *OK*.

The upload may take a few minutes to complete.

Automatic updates

The FortiGate unit can be configured to request updates from the FortiGuard Distribution Network. You can configure this to be on a scheduled basis, or with push notifications.

Scheduling updates

Scheduling updates ensures that the virus and IPS definitions are downloaded to your FortiGate unit on a regular basis, ensuring that you do not forget to check for the definition files yourself. As well, by scheduling updates during off-peak hours, such as evenings or weekends, when network usage is minimal, ensures that the network activity will not suffer from the added traffic of downloading the definition files.

If you require the most up-to-date definitions as viruses and intrusions are found in the wild, the FortiGuard Distribution Network can push updates to the FortiGate units as they are developed. This ensures that your network will be protected from any breakouts of a virus within the shortest amount of time, minimizing any damaging effect that can occur. Push updates require that you have registered your FortiGate unit.

Once push updates are enabled, the next time new antivirus or IPS attack definitions are released, the FDN notifies all the FortiGate unit that a new update is available. Within 60 seconds of receiving a push notification, the unit automatically requests the update from the FortiGuard servers.

To enable scheduled updates - web-based manager

1. Go to *System* > *Config* > *FortiGuard*.
2. Click the Expand Arrow for *AV and IPS Options*.
3. Select the *Scheduled Update* check box.
4. Select the frequency of the updates and when within that frequency.
5. Select *Apply*.

To enable scheduled updates - CLI

```
config system autoupdate schedule
  set status enable
  set frequency {every | daily | weekly}
  set time <hh:mm>
  set day <day_of_week>
end
```

Push updates

Push updates enable you to get immediate updates when new virus or intrusions have been discovered and new signatures are created. This ensures that when the latest signature is available it will be sent to the FortiGate.

When a push notification occurs, the FortiGuard server sends a notice to the FortiGate unit that there is a new signature definition file available. The FortiGate unit then initiates a download of the definition file, similar to the scheduled update.

To ensure maximum security for your network, you should have a scheduled update as well as enable the push update, in case an urgent signature is created, and your cycle of the updates only occurs weekly.

To enable push updates - web-based manager

1. Got to *System* > *Config* > *FortiGuard*.
2. Click the Expand Arrow for *AV and IPS Options*.
3. Select *Allow Push Update*.
4. Select *Apply*.

To enable push updates - CLI

```
config system autoupdate push-update
  set status enable
end
```

Push IP override

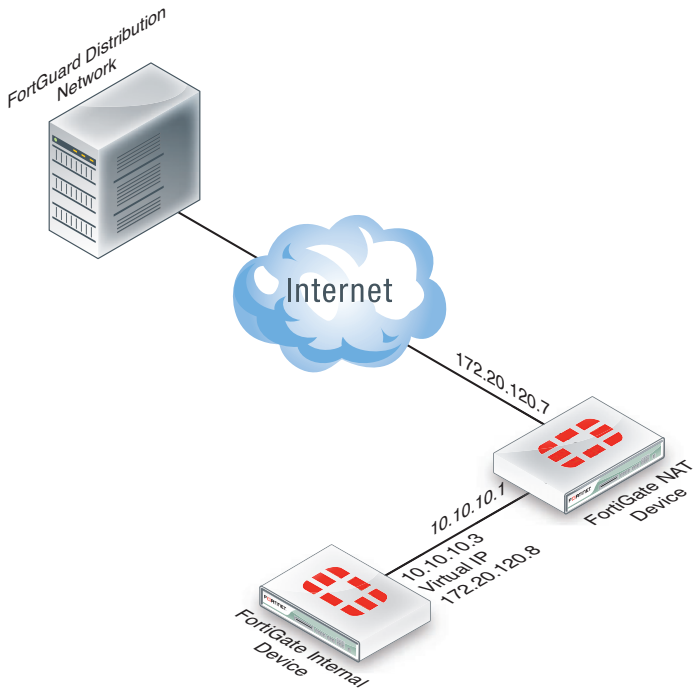
If the FortiGate unit is behind another NAT device (or another FortiGate unit), to ensure it receives the push update notifications, you need to use an override IP address for the notifications. To do this, you create a virtual IP to map to the external port of the NAT device.

Generally speaking, if there are two FortiGate devices as in the diagram below, the following steps need to be completed on the FortiGate NAT device to ensure the FortiGate unit on the internal network receives the updates:

- Add a port forwarding virtual IP to the FortiGate NAT device that connects to the Internet by going to *Firewall Objects* > *Virtual IP*.
- Add a security policy to the FortiGate NAT device that connects to the Internet that includes the port forwarding virtual IP.
- Configure the FortiGate unit on the internal network with an override push IP and port.

On the FortiGate internal device, the virtual IP is entered as the *Use push override IP* address.

Figure 8: Using a virtual IP for a FortiGate unit behind a NAT device



To enable push update override- web-based manager

1. Got to *System* > *Config* > *FortiGuard*.
2. Click the Expand Arrow for *AV and IPS Options*.
3. Select *Allow Push Update*.
4. Select *Use push override IP*.
5. Enter the virtual IP address configured on the NAT device.
6. Select *Apply*.

To enable push updates - CLI

```
config system autoupdate push-update
  set status enable
  set override enable
  set address <vip_address>
end
```

Web filtering

The multiple FortiGuard data centers around the world hold the entire categorized URL database and receive rating requests from customer-owned FortiGate units, typically triggered by browser-based URL requests. When these rating requests are responded to with the categories stored for specific URLs, the requesting FortiGate unit will then use its own local profile configuration to determine what action to take, for example blocking, monitoring, or permitting the URL request.

Rating responses can also be cached locally on the FortiGate unit, providing a quicker response time while easing load on the FortiGuard servers and aiding in a quicker response time for less common URL requests. This is a very effective method for common sites such as search

engines and other frequently visited sites. Other sites that are less frequently visited can also be cached locally for a determined amount of time.

By default, the web filtering cache is enabled. The cache includes a time-to-live value, which is the amount of time a URL will stay in the cache before expiring. You can change this value to shorten or extend the time between 300 and 86400 seconds. For a site such as Google, the frequency of its access can keep it in the cache, while other sites can remain in the cache up to 24 hours, or less depending on the configuration.

Web Filtering and Email Filtering Options

Go to *System* > *Config* > *FortiGuard*, and expand arrow to view *Web Filtering and Email Filtering Options* for setting the size of the caches and ports used.

Web Filter cache TTL	Set the Time To Live value. This is the number of seconds the FortiGate unit will store a blocked IP or URL locally, saving time and network access traffic, checking the FortiGuard server. Once the TTL has expired, the FortiGate unit will contact an FDN server to verify a web address. The TTL must be between 300 and 86400 seconds.
Antispam cache TTL	Set the Time To Live value. This is the number of seconds the FortiGate unit will store a blocked IP or URL locally, saving time and network access traffic, checking the FortiGuard server. Once the TTL has expired, the FortiGate unit will contact an FDN server to verify a web address. The TTL must be between 300 and 86400 seconds.
Port Section	Select the port assignments for contacting the FortiGuard servers. Select the *Test Availability* button to verify the connection using the selected port.
To have a URL's category rating re-evaluated, please click here	Select to re-evaluate a URL's category rating on the FortiGuard Web Filter service.

URL verification

If you discover a URL - yours or one you require access to has been incorrectly flagged as an inappropriate site - you can ask the FortiGuard team to re-evaluate the site. To do this, go to *System* > *Config* > *FortiGuard*, select the blue arrow for *Web Filtering and Email Filtering Options* and select the link for re-evaluation.

To modify the web filter cache size - web-based manager

1. Got to *System* > *Config* > *FortiGuard*.
2. Click the Expand Arrow for *Web Filtering and Email Filtering Options*.
3. Enter the TTL value for the *Web filter cache*.
4. Select *Apply*.

To modify the web filter cache size - CLI

```
config system fortiguard
  set webfilter-cache-ttl <integer>
end
```

Further web filtering options can be configured to block specific URLs, and allow others through. These configurations are available through the *Security Profiles* > *Web Filter* menu. For more information, see *Security* chapter of The Handbook.

Email filtering

The FortiGuard data centers monitor and update email databases of known spam sources. With FortiGuard Antispam enabled, the FortiGate unit verifies incoming email sender address and IPs against the database, and take the necessary action as defined within the antivirus profiles.

Spam source IP addresses can also be cached locally on the FortiGate unit, providing a quicker response time, while easing load on the FortiGuard servers, aiding in a quicker response time for less common email address requests.

By default, the antispam cache is enabled. The cache includes a time-to-live value, which is the amount of time an email address will stay in the cache before expiring. You can change this value to shorten or extend the time between 300 and 86400 seconds.

To modify the antispam filter cache size - web-based manager

1. Got to *System* > *Config* > *FortiGuard*.
2. Click the Expand Arrow for *Web Filtering and Email Filtering Options*.
3. Enter the TTL value for the *antispam cache*.
4. Select *Apply*.

To modify the web filter cache size - CLI

```
config system fortiguard
  set antispam-cache-ttl <integer>
end
```

Further antispam filtering options can be configured to block, allow or quarantine, specific email addresses. These configurations are available through the *Security Profiles* > *Antispam* menu. For more information, see *Security Profiles* chapter of The Handbook.

Security tools

The FortiGuard online center provides a number of online security tools that enable you to verify or check ratings of web sites, email addresses as well as check file for viruses. These features are available at http://www.fortiguard.com.

URL lookup

By entering a web site address, you can see if it has been rated and what category and classification it is filed as. If you find your web site or a site you commonly go to has been wrongly categorized, you can use this page to request that the site be re-evaluated.

http://www.fortiguard.com/webfiltering/webfiltering.html

IP and signature lookup

The IP and signature lookup enables you to check whether an IP address is blacklisted in the FortiGuard IP reputation database or whether a URL or email address is in the signature database.

http://www.fortiguard.com/antispam/antispam.html

Online virus scanner

If you discover a suspicious file on your machine, or suspect that a program you downloaded from the Internet might be malicious you can scan it using the FortiGuard online scanner. The questionable file can be uploaded from your computer to a dedicated server where it will be scanned using FortiClient Antivirus. Only one file of up to 1 MB can be checked at any one time. All files will be forwarded to our research labs for analysis.

http://www.fortiguard.com/antivirus/virus_scanner.html

Malware removal tools

Tools have been developed by FortiGuard Labs to disable and remove the specific malware and related variants. Some tools have been developed to remove specific malware, often tough to remove. A universal cleaning tool, FortiCleanup, is also available for download.

The FortiCleanup is a tool developed to identify and cleanse systems of malicious rootkit files and their associated malware. Rootkits consist of code installed on a system with kernel level privileges, often used to hide malicious files, keylog and thwart detection / security techniques. The aim of this tool is to reduce the effectiveness of such malware by finding and eliminating rootkits. The tool offers a quick memory scan as well as a full system scan. FortiCleanup will not only remove malicious files, but also can cleanse registry entries, kernel module patches, and other tricks commonly used by rootkits - such as SSDT hooks and process enumeration hiding.

A license to use these applications is provided free of charge, courtesy of Fortinet.

http://www.fortiguard.com/antivirus/malware_removal.html

FortiSandbox

A FortiSandbox unit can be used for automated sample tracking, or sandboxing, for files from a FortiGate unit. This allows suspicious files to be sent to be inspected without risking network security. If the file exhibits risky behavior, or is found to contain a virus, a new virus signature is created and added to the FortiGuard antivirus signature database.

Cloud Sandbox can also be used for sandboxing if you have an active FortiCloud subscription. For more information, see “FortiCloud” on page 102.

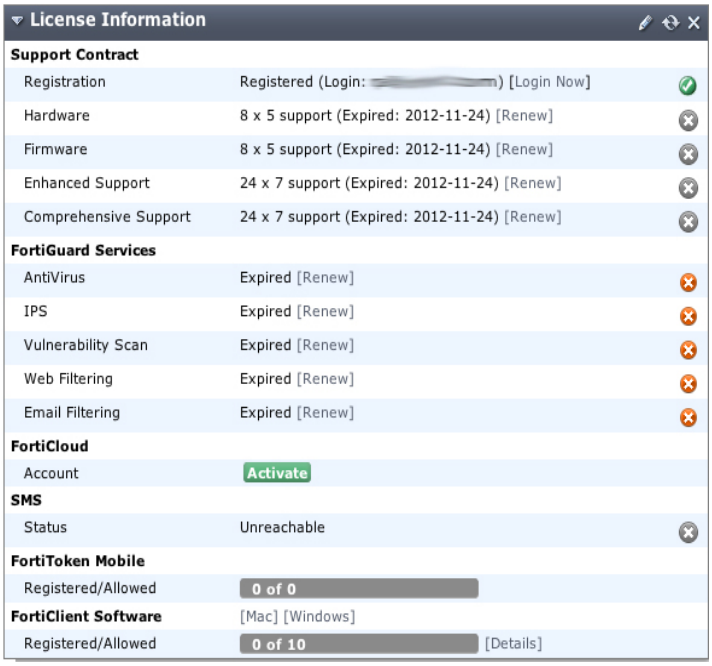
Troubleshooting

If you are not getting FortiGuard web filtering or antispam services, there are a few things to verify communication to the FortiGuard Distribution Network (FDN) is working. Before any troubleshooting, ensure that the FortiGate unit has been registered and you or your company, has subscribed to the FortiGuard services.

Web-based manager verification

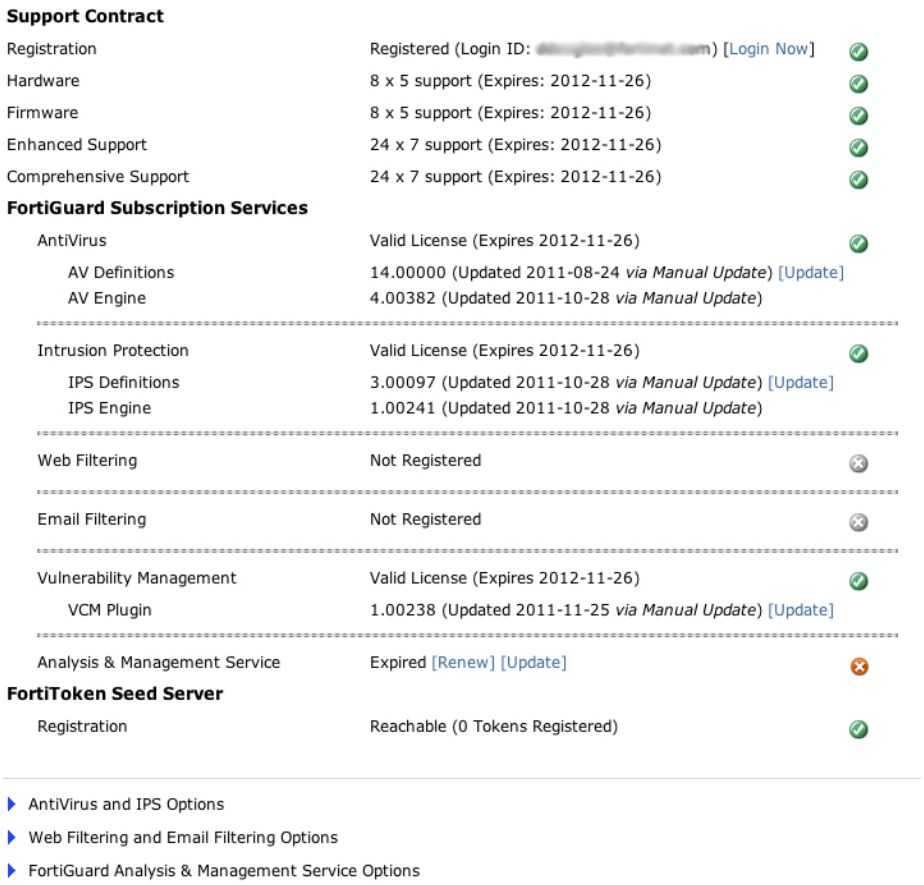
The simplest method to check that the FortiGate unit is communicating with the FDN, is to check the *License Information* dashboard widget. Any subscribed services should have a green check mark beside them indicating that connections are successful. Any other icon indicates a problem with the connection, or you are not subscribed to the FortiGuard services.

Figure 9: License Information widget showing FortiGuard availability



You can also view the FortiGuard connection status by going to *System* > *Config* > *FortiGuard*.

Figure 10: FortiGuard availability



CLI verification

You can also use the CLI to see what FortiGuard servers are available to your FortiGate unit. Use the following CLI command to ping the FDN for a connection:

```
ping guard.fortinet.net
```

You can also use diagnose command to find out what FortiGuard servers are available:

```
diagnose debug rating
```

From this command, you will see output similar to the following:

```
Locale       : english
License      : Contract
Expiration   : Sun Jul 24 20:00:00 2011
Hostname     : service.fortiguard.net

-=- Server List (Tue Nov  2 11:12:28 2010) -=-

IP Weight    RTT Flags  TZ    Packets  Curr Lost Total Lost
69.20.236.180 0     10        -5      77200          0         42
69.20.236.179 0     12        -5      52514          0         34
66.117.56.42 0     32        -5      34390          0         62
80.85.69.38 50    164         0      34430          0        11763
208.91.112.194 81    223 D      -8      42530          0       8129
216.156.209.26 286    241 DI     -8      55602          0      21555
```

An extensive list of servers are available. Should you see a list of three to five available servers, the FortiGuard servers are responding to DNS replies to service.FortiGuard.net, but the INIT requests are not reaching FDS services on the servers.

The rating flags indicate the server status:

D	Indicates the server was found via the DNS lookup of the hostname. If the hostname returns more than one IP address, all of them will be flagged with 'D' and will be used first for INIT requests before falling back to the other servers.
I	Indicates the server to which the last INIT request was sent
F	The server has not responded to requests and is considered to have failed.
T	The server is currently being timed.

The server list is sorted first by weight and then the server with the smallest RTT is put at the top of the list, regardless of weight. When a packet is lost, it will be resent to the next server in the list.

The weight for each server increases with failed packets and decreases with successful packets. To lower the possibility of using a faraway server, the weight is not allowed to dip below a base weight, which is calculated as the difference in hours between the FortiGate unit and the server multiplied by 10. The further away the server is, the higher its base weight and the lower in the list it will appear.

Port assignment

FortiGate units contact the FortiGuard Distribution Network (FDN) for the latest list of FDN servers by sending UDP packets with typical source ports of 1027 or 1031, and destination ports of 53 or 8888. The FDN reply packets have a destination port of 1027 or 1031.

If your ISP blocks UDP packets in this port range, the FortiGate unit cannot receive the FDN reply packets. As a result, the FortiGate unit will not receive the complete FDN server list.

If your ISP blocks the lower range of UDP ports (around 1024), you can configure your FortiGate unit to use higher-numbered ports, using the CLI command…

```
config system global
  set ip-src-port-range <start port>-<end port>
end
```

…where the `<start port>` and `<end port>` are numbers ranging of 1024 to 25000.

For example, you could configure the FortiGate unit to not use ports lower than 2048 or ports higher than the following range:

```
config system global
  set ip-src-port-range 2048-20000
end
```

Trial and error may be required to select the best source port range. You can also contact your ISP to determine the best range to use. Push updates might be unavailable if:

- there is a NAT device installed between the unit and the FDN
- your unit connects to the Internet using a proxy server.

FortiCloud

FortiCloud is a hosted security management and log retention service for FortiGate products. It gives you a centralized reporting, traffic analysis, configuration and log retention without the need for additional hardware and software.

FortiCloud Features

FortiCloud offers a wide range of features:

Simplified central management for your FortiGate network

FortiCloud provides a central web-based management console to manage individual or aggregated FortiGate and FortiWifi devices. Adding a device to the FortiCloud management subscription is straightforward and provides detailed traffic and application visibility across the whole network.

Hosted log retention with large default storage allocated

Log retention is an integral part of any security and compliance program but administering a separate storage system is burdensome. FortiCloud takes care of this automatically and stores the valuable log information in the cloud. Each device is allowed up to 200Gb of log retention storage. Different types of logs can be stored including Traffic, System Events, Web, Applications and Security Events.

Monitoring and alerting in real time

Network availability is critical to a good end-user experience. FortiCloud enables you to monitor your FortiGate network in real time with different alerting mechanisms to pinpoint potential issues. Alerting mechanisms can be delivered via email.

Customized or pre-configured reporting and analysis tools

Reporting and analysis are your eyes and ears into your network's health and security. Pre-configured reports are available, as well as custom reports that can be tailored to your specific reporting and compliance requirements. For example, you may want to look closely at application usage or web site violations. The reports can be emailed as PDFs and can cover different time periods.

Maintain important configuration information uniformly

The correct configuration of the devices within your network is essential to maintaining an optimum performance and security posture. In addition, maintaining the correct firmware (operating system) level allows you to take advantage of the latest features.

Service security

All communication (including log information) between the devices and the clouds is encrypted. Redundant data centers are always used to give the service high availability. Operational

security measures have been put in place to make sure your data is secure — only you can view or retrieve it.

Registration and Activation

There are five key activation steps. The procedure for each step may vary depending on your model and your FortiOS firmware version, and whether your device (FortiGate or FortiWifi) is brand new.

The steps are:

1. Registering with Support (New devices only)
2. Activating your FortiCloud account
3. Enabling logging to FortiCloud
4. Logging into the FortiCloud portal
5. Upgrading to a 200Gb subscription (Recommended)

Registering with Support

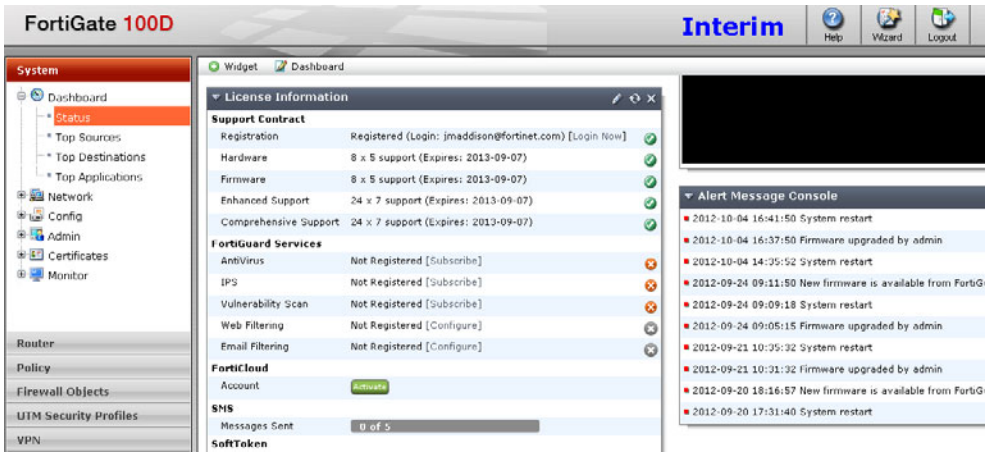
Registration is very important for new devices, as it allows interaction with the Fortinet back-end systems, such as support. This registration will also allow other services, such as support and data space expansion contracts, to be used with your FortiCloud account.

Registering and Activating your FortiCloud account

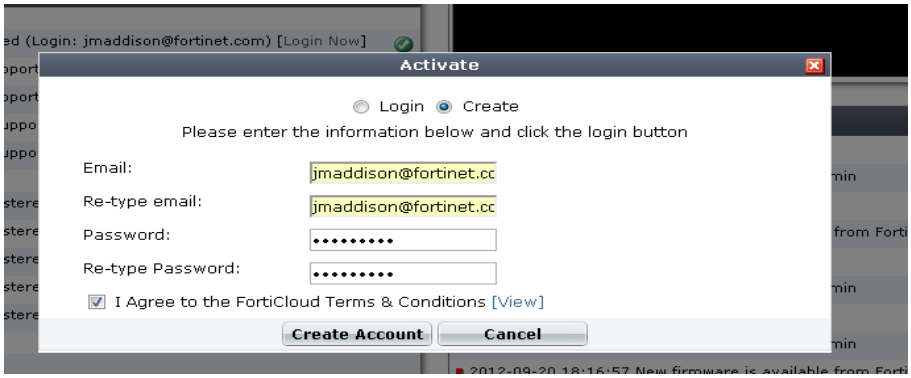
FortiCloud accounts can be registered manually through the FortiCloud website, https://www.forticloud.com, but you can easily register and activate your account directly within your FortiGate unit. Your registration process will vary somewhat, depending on which firmware version and device you have.

FortiGate 300 and below, all FortiWifi units

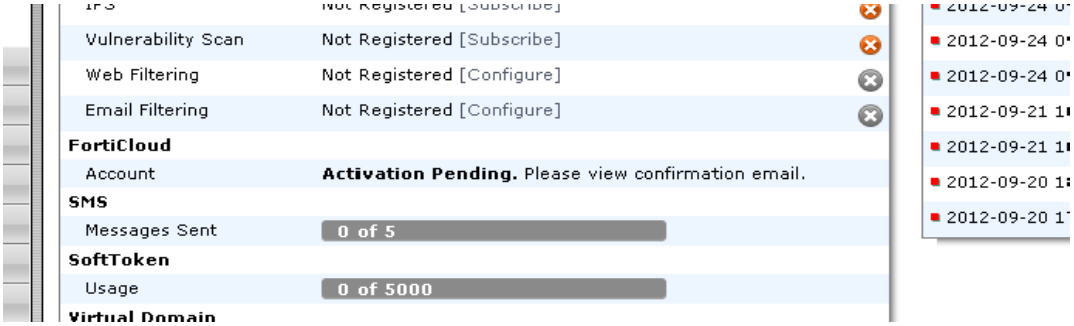
1. On your device's dashboard, in the License Information widget, select the green *Activate* button in the FortiCloud section.



2. A dialogue asking you to register your FortiCloud account will appear. Enter your information, view and accept the Terms and Conditions and select *Create Account*.



3. A second dialogue window will appear, asking you to enter your information to confirm your account. This will send a confirmation email to your registered email. The dashboard widget will update to show that confirmation is required.



4. Open your email, and follow the confirmation link contained in it.

A FortiCloud page will open, stating that your account has been confirmed. The Activation Pending message on the dashboard will change to state the type of account you have ('1Gb Free' or '200Gb Subscription'), and will now provide a link to the FortiCloud portal.

FortiGate 600 to 800

For 600 through 800, FortiCloud registration must be done through the FortiGate CLI Console.

Devices beyond the FortiGate 800 do not support the FortiCloud service.

Enabling logging to FortiCloud

In order to enable remote logging to the FortiCloud Service, you must first configure the FortiGate's log uploading settings. You must also enable logging in each policy that covers traffic that you want to be logged.

FortiOS 5.0

FortiOS 5.0 will automatically start logging Traffic and Event logs to FortiCloud upon activation. Logging can be disabled or configured through the FortiGate interface or CLI Console.

Configuring policies 5.0

After enabling logging functionality, you will need to select which policies will be logged.

1. Open the Policy list.
2. Choose the policy you would like to log, and select *Edit*.
3. Check the box next to *Log all sessions*.
4. Select *OK*.

Logging into the FortiCloud portal

Once logging has been configured and you have registered your account, you can log into the FortiCloud portal and begin viewing your logging results. There are two methods to reach the FortiCloud portal:

- If you have direct networked access to the FortiGate unit, you can simply open your Dashboard and check the License Information widget. Next to the current FortiCloud connection status will be a link to reach the FortiCloud Portal.
- If you do not currently have access to the FortiGate's interface, you can visit the FortiCloud website (https://forticloud.com) and log in remotely, using your email and password. It will ask you to confirm the FortiCloud account you are connecting to and then you will be granted access. Connected devices can be remotely configured using the Scripts page in the Management Tab, useful if an administrator may be away from the unit for a long period of time.

Upgrading to a 200Gb subscription

Upgrading your subscription is simple but must be done through the FortiGate unit, as the storage contract is allocated based on devices rather than user accounts.

1. Open the FortiGate Dashboard.
2. In the License Information widget, select *Upgrade* next to 'Type' in the FortiCloud section.
3. A new window will open, showing the Fortinet Support portal. Follow the on-screen instructions to register your contract.
4. Wait approximately 10 minutes for the contract to be applied and then visit your Dashboard.

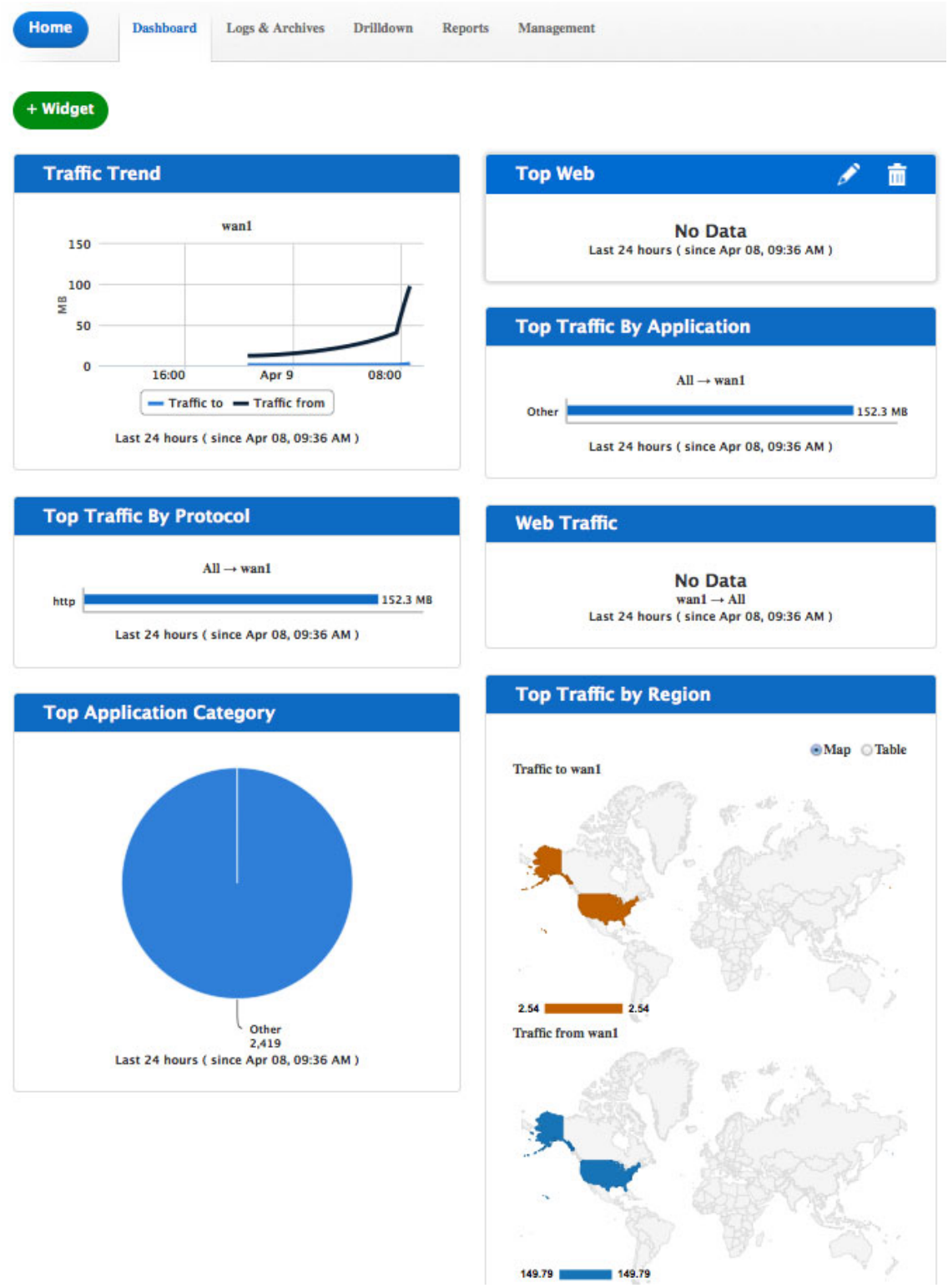
In the License Information widget, Type will have changed from 'Free' to 'Subscribed'. Your maximum listed storage will also have updated.

The FortiCloud Portal

There are five main tabs in the FortiCloud portal, which allow you to access different features and information. The FortiCloud Settings, Help, and Logout buttons appear in the upper right.

- Dashboards
- Logs & Archives
- Drilldown
- Reports
- Management
- AV Submissions (this tab only appears if sandboxing has occurred, see "Cloud Sandboxing" on page 107)

Figure 11: The FortiCloud Portal



Using FortiCloud

Below is a list of possible tasks that show you how to make the best of the features that FortiCloud has to offer.

Tasks:

- Adding a new dashboard with custom charts
- Filtering logs to find specific information
- Downloading logs
- Using drilldown charts to find specific information
- Viewing and printing existing reports
- Generating scheduled and immediate reports
- Creating and configuring a new report with your logo
- Checking the status of your registration contract
- Adding a new user account to a FortiCloud account

For further information about using FortiCloud, please see the *FortiCloud Getting Started Guide*.

Cloud Sandboxing

FortiCloud can be used for automated sample tracking, or sandboxing, for files from a FortiGate unit. This allows suspicious files to be sent to be inspected without risking network security. If the file exhibits risky behavior, or is found to contain a virus, a new virus signature is created and added to the FortiGuard antivirus signature database. This feature was formerly known as FortiGuard Analytics.

Cloud sandboxing is configured by going to *System* > *Config* > *FortiSandbox*. After enabling FortiSandbox, select *Cloud Sandbox (FortiCloud).*

Sandboxing results will be shown in a new tab called *AV Submissions* in the FortiCloud portal. This tab will only appear after a file has been sent for sandboxing.

Interfaces

Interfaces, both physical and virtual, enable traffic to flow to and from the internal network, and the Internet and between internal networks. The FortiGate unit has a number of options for setting up interfaces and groupings of subnetworks that can scale to a company's growing requirements.

This chapter includes:

Physical

FortiGate units have a number of physical ports where you connect ethernet or optical cables. Depending on the model, they can have anywhere from four to 40 physical ports. Some units have a grouping of ports labelled as internal, providing a built-in switch functionality.

In FortiOS, the port names, as labeled on the FortiGate unit, appear in the web-based manager in the *Unit Operation* widget, found on the Dashboard. They also appear when you are configuring the interfaces, by going to *System* > *Network* > *Interface*. As shown below, the FortiGate-100D (Generation 2) has 22 interfaces.

Two of the physical ports on the FortiGate-100D (Generation 2) are SFP ports. These ports share the numbers 15 and 16 with RJ-45 ports. Because of this, when SFP port 15 is used, RJ-45 port 15 cannot be used, and vice versa.

These ports also share the same MAC address.

Figure 12: FortiGate-100D physical interfaces

Figure 13: FortiGate-100D interfaces on the Dashboard

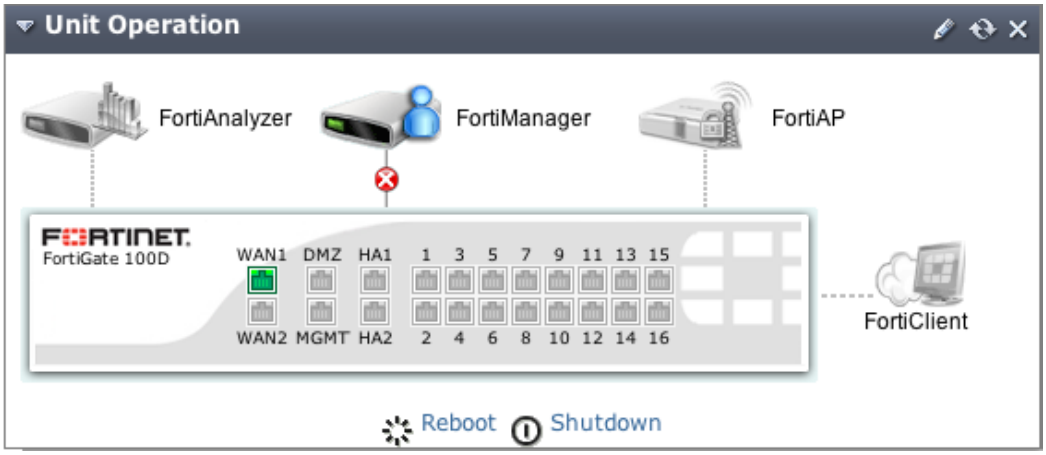


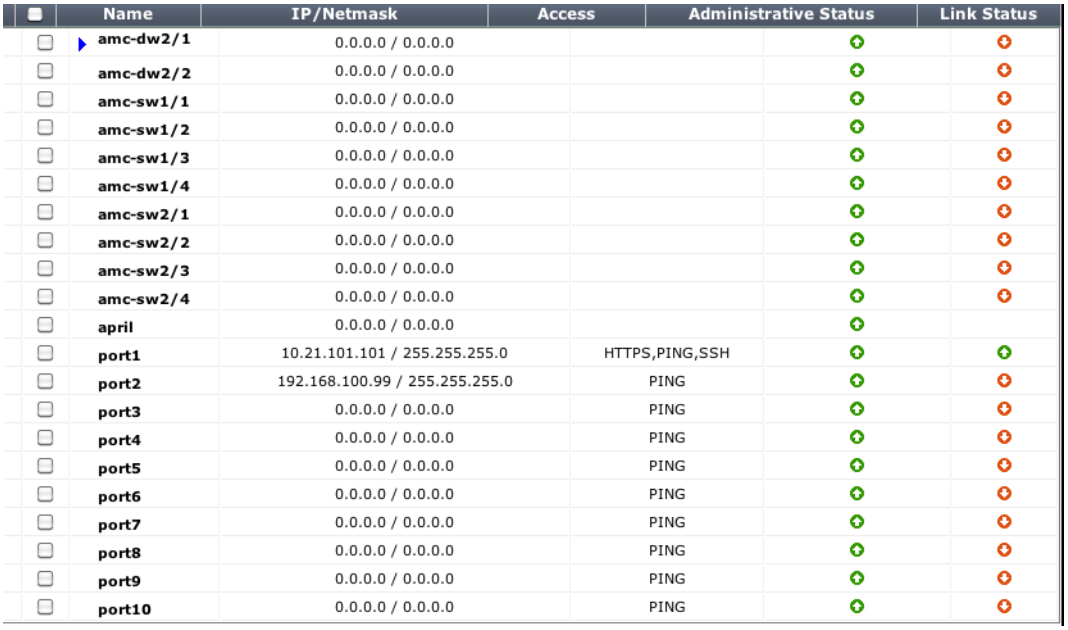
Figure 14: Configuring the FortiGate-100D ports

	Name	Type	IP/Netmask	Access	Administrative Status	Link Status	Ref.
	wan1	Physical	172.20.120.230 / 255.255.255.0	HTTP,HTTPS,PING,SSH		100 Mbps/Full Duplex	1
	dmz	Physical	10.10.10.1 / 255.255.255.0	HTTPS,PING,FMG-Access			1
	modem	Physical	0.0.0.0 / 0.0.0.0				0
	wan2	Physical	0.0.0.0 / 0.0.0.0	PING,FMG-Access			1
	mgmt	Physical	192.168.1.99 / 255.255.255.0	HTTPS,PING,FMG-Access			0
	ha1	Physical	0.0.0.0 / 0.0.0.0				0
	ha2	Physical	0.0.0.0 / 0.0.0.0				0
	internal	Physical	192.168.100.99 / 255.255.255.0	HTTPS,PING,FMG-Access		100 Mbps/Full Duplex	3

Normally the internal interface is configured as a single interface shared by all physical interface connections - a switch. The switch mode feature has two states - switch mode and interface mode. Switch mode is the default mode with only one interface and one address for the entire internal switch. Interface mode enables you to configure each of the internal switch physical interface connections separately. This enables you to assign different subnets and netmasks to each of the internal physical interface connections.

The larger FortiGate units can also include Advanced Mezzanine Cards (AMC), which can provide additional interfaces (Ethernet or optical), with throughput enhancements for more efficient handling of specialized traffic. These interfaces appear in FortiOS as port amc/sw1, amc/sw2 and so on. In the following illustration, the FortiGate-3810A has three AMC cards installed: two single-width (amc/sw1, amc/sw2) and one double-width (amc/dw).

Figure 15: FortiGate-3810A AMC card port naming



Name	IP/Netmask	Access	Administrative Status	Link Status
amc-dw2/1	0.0.0.0 / 0.0.0.0			
amc-dw2/2	0.0.0.0 / 0.0.0.0			
amc-sw1/1	0.0.0.0 / 0.0.0.0			
amc-sw1/2	0.0.0.0 / 0.0.0.0			
amc-sw1/3	0.0.0.0 / 0.0.0.0			
amc-sw1/4	0.0.0.0 / 0.0.0.0			
amc-sw2/1	0.0.0.0 / 0.0.0.0			
amc-sw2/2	0.0.0.0 / 0.0.0.0			
amc-sw2/3	0.0.0.0 / 0.0.0.0			
amc-sw2/4	0.0.0.0 / 0.0.0.0			
april	0.0.0.0 / 0.0.0.0			
port1	10.21.101.101 / 255.255.255.0	HTTPS,PING,SSH		
port2	192.168.100.99 / 255.255.255.0	PING		
port3	0.0.0.0 / 0.0.0.0	PING		
port4	0.0.0.0 / 0.0.0.0	PING		
port5	0.0.0.0 / 0.0.0.0	PING		
port6	0.0.0.0 / 0.0.0.0	PING		
port7	0.0.0.0 / 0.0.0.0	PING		
port8	0.0.0.0 / 0.0.0.0	PING		
port9	0.0.0.0 / 0.0.0.0	PING		
port10	0.0.0.0 / 0.0.0.0	PING		

Interface settings

In *System* > *Network* > *Interface*, you configure the interfaces, physical and virtual, for the FortiGate unit. There are different options for configuring interfaces when the FortiGate unit is in NAT mode or transparent mode. On FortiOS Carrier, you can also enable the Gi gatekeeper on each interface for anti-overbilling.

Interface page	
Create New	Select to add a new interface, zone or, in transparent mode, port pair. For more information on configuring zones, see Zones. Depending on the model you can add a VLAN interface, a loopback interface, a IEEE 802.3ad aggregated interface, or a redundant interface. When VDOMs are enabled, you can also add Inter-VDOM links.
Name	The names of the physical interfaces on your FortiGate unit. This includes any alias names that have been configured. When you combine several interfaces into an aggregate or redundant interface, only the aggregate or redundant interface is listed, not the component interfaces. If you have added VLAN interfaces, they also appear in the name list, below the physical or aggregated interface to which they have been added. If you have added loopback interfaces, they also appear in the interface list, below the physical interface to which they have been added. If you have software switch interfaces configured, you will be able to view them. For more information, see “Software switch” on page 114. If your FortiGate unit supports AMC modules, the interfaces are named amc-sw1/1, amc-dw1/2, and so on.
Type	The configuration type for the interface.

IP/Netmask	The current IP address and netmask of the interface. In VDOM mode, when VDOMs are not all in NAT or transparent mode some values may not be available for display and will be displayed as "-".
Access	The administrative access configuration for the interface.
Administrative Status	Indicates if the interface can be accessed for administrative purposes. If the administrative status is a green arrow, and administrator could connect to the interface using the configured access. If the administrative status is a red arrow, the interface is administratively down and cannot be accessed for administrative purposes.
Link Status	The status of the interface physical connection. Link status can be either up (green arrow) or down (red arrow). If link status is up the interface is connected to the network and accepting traffic. If link status is down the interface is not connected to the network or there is a problem with the connection. You cannot change link status from the web-based manager, and typically is indicative of an ethernet cable plugged into the interface. Link status is only displayed for physical interfaces.
MAC	The MAC address of the interface.
Mode	Shows the addressing mode of the interface. The addressing mode can be manual, DHCP, or PPPoE.
Secondary IP	Displays the secondary IP addresses added to the interface.
MTU	The maximum number of bytes per transmission unit (MTU) for the interface.
Virtual Domain	The virtual domain to which the interface belongs. This column is visible when VDOM configuration is enabled.
VLAN ID	The configured VLAN ID for VLAN subinterfaces.

Interface configuration and settings

To configure an interface, go to *System* > *Network* > *Interface and* select *Create New*.

Name	Enter a name of the interface. Physical interface names cannot be changed.
Alias	Enter an alternate name for a physical interface on the FortiGate unit. This field appears when editing an existing physical interface. The alias can be a maximum of 25 characters. The alias name will not appears in logs.
Link Status	Indicates whether the interface is connected to a network (link status is *Up*) or not (link status is *Down*). This field appears when editing an existing physical interface.
Type	Select the type of interface that you want to add. On some models you can set *Type* to *802.3ad Aggregate* or *Redundant Interface*.

Interface	Displayed when *Type* is set to *VLAN*. Select the name of the physical interface to which to add a VLAN interface. Once created, the VLAN interface is listed below its physical interface in the Interface list. You cannot change the physical interface of a VLAN interface except when adding a new VLAN interface.
VLAN ID	Displayed when *Type* is set to *VLAN*. Enter the VLAN ID. You cannot change the *VLAN ID* except when adding a new VLAN interface. The VLAN ID can be any number between 1 and 4094 and must match the VLAN ID added by the IEEE 802.1Q-compliant router or switch connected to the VLAN subinterface.
Virtual Domain	Select the virtual domain to add the interface to. Admin accounts with super_admin profile can change the *Virtual Domain*.
Physical Interface Members	This section has two different forms depending on the interface type: • **Software switch interface** - this section is a display-only field showing the interfaces that belong to the software switch virtual interface. • **802.3ad aggregate or Redundant interface** - this section includes available interface and selected interface lists to enable adding or removing interfaces from the interface. For more information, see Redundant interfaces. Select interfaces from this *Available Interfaces* list and select the right arrow to add an interface to the *Selected Interface* list.
Addressing mode	Select the addressing mode for the interface. • Select *Manual* and add an *IP/Netmask* for the interface. If IPv6 configuration is enabled you can add both a IPv4 and an IPv6 IP address. • Select *DHCP* to get the interface IP address and other network settings from a DHCP server. For more information, see DHCP addressing mode on an interface • Select *PPPoE* to get the interface IP address and other network settings from a PPPoE server. For more information, see PPPoE addressing mode on an interface. • Select *One-Arm Sniffer* to enable the interface as a means to detect possible traffic threats. This option is available on physical ports not configured for the primary Internet connection. For more information see One-armed sniffer. • Select *Dedicate to FortiAP/FortiSwitch* to have a FortiAP unit or FortiSwitch unit connect exclusively to the interface. This option is only available when editing a physical interface, and it has a static IP address. When you enter the IP address, the FortiGate unit automatically creates a DHCP server using the subnet entered. This option is not available on the ADSL interface. The FortiSwitch option is currently only available on the FortiGate-100D.

IP/Netmask	If *Addressing Mode* is set to *Manual*, enter an IPv4 address/subnet mask for the interface. FortiGate interfaces cannot have IP addresses on the same subnet.
IPv6 Address	If *Addressing Mode* is set to *Manual* and IPv6 support is enabled, enter an IPv6 address/subnet mask for the interface. A single interface can have both an IPv4 and IPv6 address or just one or the other.
Administrative Access	Select the types of administrative access permitted for IPv4 connections to this interface.
HTTPS	Allow secure HTTPS connections to the web-based manager through this interface. If configured, this option will enable automatically when selecting the *HTTP* option. For information on this setting, see "HTTPS redirect" on page 66.
PING	Interface responds to pings. Use this setting to verify your installation and for testing.
HTTP	Allow HTTP connections to the web-based manager through this interface. If configured, this option will also enable the *HTTPS* option. For information on this setting, see "HTTPS redirect" on page 66.
SSH	Allow SSH connections to the CLI through this interface.
SNMP	Allow a remote SNMP manager to request SNMP information by connecting to this interface.
TELNET	Allow Telnet connections to the CLI through this interface. Telnet connections are not secure and can be intercepted by a third party.
FMG-Access	Allow FortiManager authorization automatically during the communication exchange between the FortiManager and FortiGate units.
FCT-Access	You can configure a FortiGate interface as an interface that will accept FortiClient connections. When configured, the FortiGate unit sends broadcast messages which the FortiClient software running on a end user PC is listening for.
CAPWAP	Allows the FortiGate unit's wireless controller to manage a wireless access point, such as a FortiAP unit.
IPv6 Administrative Access	Select the types of administrative access permitted for IPv6 connections to this interface. These types are the same as for Administrative Access.
Security Mode	Select a captive portal for the interface. When selected, you can define the portal message and look that the user sees when logging into the interface. You can also define one or more user groups that have access to the interface.
DHCP Server	Select to enable a DHCP server for the interface. For more information on configuring a DHCP server on the interface, see "DHCP servers and relays" on page 205.
Detect and Identify Devices	Select to enable the interface to be used with BYOD hardware such as iPhones. Define the device definitions by going to *User & Device* > *Device*.

Add New Devices to Vulnerability Scan List	This option appears when *Detect and Identify Devices* is enabled. When enabled, the FortiGate unit performs a network vulnerability scan of any devices detected or seen on the interface. The vulnerability scan occur as configured, either on demand, or as scheduled.
Broadcast Discovery Messages	Available when *FCT-Access* is enabled for the *Administrative Access*. Select to enable sends broadcast messages which the FortiClient software running on a end user PC is listening for. Once enabled, the FortiGate unit broadcasts a discovery message that includes the IP address of the interface and listening port number to the local network. All PCs running FortiClient on that network listen for this discovery message.
Enable Explicit Web Proxy	Available when enabling explicit proxy on the *System Information* Dashboard (*System* > *Dashboard* > *Status*). This option is not available for a VLAN interface selection. Select to enable explicit web proxying on this interface. When enabled, this interface will be displayed on *System* > *Network* > *Explicit Proxy* under *Listen on Interfaces* and web traffic on this interface will be proxied according to the Web Proxy settings.
Enable STP	With FortiGate units with a switch interface is in switch mode, this option is enabled by default. It enables the single instance MSTP spanning tree protocol.
Listen for RADIUS Accounting Messages	Select to use the interface as a listening port for RADIUS content.
Secondary IP Address	Add additional IPv4 addresses to this interface. Select the Expand Arrow to expand or hide the section.
Comments	Enter a description up to 63 characters to describe the interface.
Administrative Status	Select either *Up* (green arrow) or *Down* (red arrow) as the status of this interface. *Up* indicates the interface is active and can accept network traffic. *Down* indicates the interface is not active and cannot accept traffic.
Gi Gatekeeper (FortiOS Carrier only)	For FortiOS Carrier, enable Gi Gatekeeper to enable the Gi firewall as part of the anti-overbilling configuration. You must also configure *Gi Gatekeeper Settings* by going to *System* > *Admin* > *Settings*.

Software switch

A software switch, or soft switch, is a virtual switch that is implemented at the software, or firmware level, rather than the hardware level. A software switch can be used to simplify communication between devices connected to different FortiGate interfaces. For example, using a software switch, you can place the FortiGate interface connected to an internal network on the same subnet as your wireless interfaces. Then devices on the internal network can communicate with devices on the wireless network without any additional configuration such as additional security policies, on the FortiGate unit.

It can also be useful if you require more hardware ports on for the switch on a FortiGate unit. For example, if your FortiGate unit has a 4-port switch, WAN1, WAN2 and DMZ interfaces, and you need one more port, you can create a soft switch that can include the 4-port switch and the DMZ interface all on the same subnet. These types of applications also apply to wireless interfaces and virtual wireless interfaces and physical interfaces such as those with FortiWiFi and FortiAP unit.

Similar to a hardware switch, a software switch functions like a single interface. A software switch has one IP address; all of the interfaces in the software switch are on the same subnet. Traffic between devices connected to each interface are not regulated by security policies, and traffic passing in and out of the switch are affected by the same policy.

There are a few things to consider when setting up a software switch:

- Ensure you create a back up of the configuration.
- Ensure you have at least one port or connection such as the console port to connect to the FortiGate unit. If you accidentally combine too many ports, you will need a way to undo any errors.
- The ports that you include must not have any link or relation to any other aspect of the FortiGate unit. For example, DHCP servers, security policies, and so on.
- For increased security, you can create a captive portal for the switch, allowing only specific user groups access to the resources connected to the switch.

To create a software switch - web-based manager

1. Go to *System* > *Network* > *Interface* and select *Create New*.
2. For *Type*, select *Software Switch*.
3. In the *Physical Interface Members* option, select the interfaces to include.
4. Configure the remaining interface settings
5. Select *OK*.

To create a software switch - CLI

```
config system switch-interface
  edit <switch-name>
    set type switch
    set member <interface_list>
end
config system interface
  edit <switch_name>
    set ip <ip_address>
    set allowaccess https ssh ping
end
```

Soft switch example

For this example, the wireless interface (WiFi) needs to be on the same subnet as the DMZ1 interface to facilitate wireless syncing from an iPhone and a local computer. The synching

between two subnets is problematic. By putting both interfaces on the same subnet the synching will work. The software switch will accomplish this.

In this example, the soft switch includes a wireless interface. Remember to configure any wireless security before proceeding. If you leave this interface open without any password or other security, it leaves open access to not only the wireless interface but to any other interfaces and devices connected within the software switch.

Clear the interfaces and back up the configuration

First, ensure that the interfaces are not being used with any other security policy or other use on the FortiGate unit. Check the WiFi and DMZ1 ports to ensure DHCP is not enabled on the interface and there are no other dependencies with these interfaces.

Next, save the current configuration, in the event something doesn't work, recovery can be quick.

Merge the interfaces

The plan is to merge the WiFi port and DMZ1 port. This will create a software switch with a name of "synchro" with an IP address of 10.10.21.12. The steps will create the switch, add the IP and then set the administrative access for HTTPS, SSH and Ping.

To merge the interfaces - CLI

```
config system switch-interface
  edit synchro
    set type switch
    set member dmz1 wifi
end
config system interface
  edit synchro
    set ip 10.10.21.12
    set allowaccess https ssh ping
end
```

Final steps

With the switch set up, you can now add security policies, DHCP servers an any other configuration that you would normally do to configure interfaces on the FortiGate unit.

Virtual Switch

Virtual switch feature enables you create virtual switches on top of the physical switch(es) with designated interfaces/ports so that a virtual switch can build up its forwarding table through learning and forward traffic accordingly. When traffic is forwarded among interfaces belonging to the same virtual switch, the traffic doesn't need to go up to the software stack, but forwarded directly by the switch. When traffic has to be relayed to interfaces not on the virtual switch, the traffic will go through the normal data path and be offloaded to NP4 when possible.

This feature is only available on mid to high end FortiGate units, including the 100D, 600C, 1000C, and 1240B.

To enable and configure the virtual switch, enter the CLI commands:

```
config system virtual-switch
  edit vs1
    set physical-switch sw0
      config port
        edit 1
          set port port1
          set speed xx
          set duplex xx
          set status [up|down]
        edit 2
          set port port2
          set ...
        end
    end
end
```

Loopback interfaces

A loopback interface is a logical interface that is always up (no physical link dependency) and the attached subnet is always present in the routing table.

The FortiGate's loopback IP address does not depend on one specific external port, and is therefore possible to access it through several physical or VLAN interfaces. Multiple loopback interfaces can be configured in either non-VDOM mode or in each VDOM.

Loopback interfaces still require appropriate firewall policies to allow traffic to and from this type of interface.

A loopback interface can be used with:

- Management access
- BGP (TCP) peering
- PIM RP

Loopback interfaces are a good practice for OSPF. Setting the OSPF router ID the same as loopback IP address troubleshooting OSPF easier, and remembering the management IP addresses (telnet to “router ID”).

Dynamic routing protocols can be enabled on loopback interfaces

For black hole static route, use the black hole route type instead of the loopback interface.

Redundant interfaces

On some models you can combine two or more physical interfaces to provide link redundancy. This feature enables you to connect to two or more switches to ensure connectivity in the event one physical interface or the equipment on that interface fails.

In a redundant interface, traffic is only going over one interface at any time. This differs from an aggregated interface where traffic is going over all interfaces for distribution of increased bandwidth. This difference means redundant interfaces can have more robust configurations with fewer possible points of failure. This is important in a fully-meshed HA configuration.

An interface is available to be in a redundant interface if:

- it is a physical interface, not a VLAN interface
- it is not already part of an aggregated or redundant interface
- it is in the same VDOM as the redundant interface
- it has no defined IP address
- is not configured for DHCP or PPPoE
- it has no DHCP server or relay configured on it
- it does not have any VLAN subinterfaces
- it is not referenced in any security policy, VIP, or multicast policy
- it is not monitored by HA
- it is not one of the FortiGate-5000 series backplane interfaces

When an interface is included in a redundant interface, it is not listed on the *System* > *Network* > *Interface* page. You cannot configure the interface individually and it is not available for inclusion in security policies, VIPs, or routing.

One-armed sniffer

A one-armed sniffer is used to configure a physical interface on the FortiGate unit as a one-arm intrusion detection system (IDS). Traffic sent to the interface is examined for matches to the configured IPS sensor and application control list. Matches are logged and then all received traffic is dropped. Sniffing only reports on attacks. It does not deny or otherwise influence traffic.

Using the one-arm sniffer, you can configure a FortiGate unit to operate as an IDS appliance by sniffing network traffic for attacks without actually processing the packets. To configure one-arm IDS, you enable sniffer mode on a FortiGate interface and connect the interface to a hub or to the SPAN port of a switch that is processing network traffic.

To assign an interface as a sniffer interface, go to *System* > *Network* > *Interface*, edit the interface and select *One-Arm Sniffer*.

If the check box is not available, the interface is in use. Ensure that the interface is not selected in any firewall policies, routes, virtual IPs or other features in which a physical interface is specified.

Enable Filters	Select to include filters to define a more granular sniff of network traffic. Select specific addresses, ports, VLANs and protocols. In all cases, enter a number, or number range, for the filtering type. For Protocol values, standard protocols are: • UDP - 17 • TCP - 6 • ICMP - 1
Include IPv6 Packets	If your network is running a combination of IPv4 and IPv6 addressing, select to sniff both addressing types. Otherwise, the FortiGate unit will only sniff IPv4 traffic.

Include Non-IP Packets	Select for a more intense scan of content in the traffic.
UTM Security Profiles	IPS sensors, and application control lists enable you to select specific sensors and application you want to identify within the traffic.

Aggregate Interfaces

Link aggregation (IEEE 802.3ad) enables you to bind two or more physical interfaces together to form an aggregated (combined) link. This new link has the bandwidth of all the links combined. If a link in the group fails, traffic is transferred automatically to the remaining interfaces with the only noticeable effect being a reduced bandwidth.

This is similar to redundant interfaces with the major difference being that a redundant interface group only uses one link at a time, where an aggregate link group uses the total bandwidth of the functioning links in the group, up to eight.

Support of the IEEE standard 802.3ad for link aggregation is available on some models.

An interface is available to be an aggregate interface if:

- it is a physical interface, not a VLAN interface or subinterface
- it is not already part of an aggregate or redundant interface
- it is in the same VDOM as the aggregated interface. Aggregate ports cannot span multiple VDOMs.
- it does not have an IP address and is not configured for DHCP or PPPoE
- it is not referenced in any security policy, VIP, IP Pool or multicast policy
- it is not an HA heartbeat interface
- it is not one of the FortiGate-5000 series backplane interfaces

Some models of FortiGate units do not support aggregate interfaces. In this case, the aggregate option is not an option in the web-based manager or CLI. As well, you cannot create aggregate interfaces from the interfaces in a switch port.

To see if a port is being used or has other dependencies, use the following diagnose command:

```
diagnose sys checkused system.interface.name <interface_name>
```

When an interface is included in an aggregate interface, it is not listed on the *System* > *Network* > *Interface* page. Interfaces will still appear in the CLI, although configuration for those interfaces will not take affect. You cannot configure the interface individually and it is not available for inclusion in security policies, VIPs, IP pools, or routing.

Example

This example creates an aggregate interface on a FortiGate-3810A using ports 4-6 with an internal IP address of 10.13.101.100, as well as the administrative access to HTTPS and SSH.

To create an aggregate interface - web-based manager

1. Go to *System* > *Network* > *Interface* and select *Create New*.
2. Enter the Name as `Aggregate`.
3. For the *Type*, select *802.3ad Aggregate*.

   If this option does not appear, your FortiGate unit does not support aggregate interfaces.
4. In the *Available Interfaces* list, select port 4, 5 and 6 and move it to the *Selected Interfaces* list.

5. Select the *Addressing Mode* of *Manual*.
6. Enter the IP address for the port of 10.13.101.100/24.
7. For *Administrative Access* select HTTPS and SSH.
8. Select *OK*.

To create aggregate interface - CLI

```
config system interface
  edit Aggregate
    set type aggregate
    set member port4 port5 port6
    set vdom root
    set ip 172.20.120.100/24
    set allowaccess https ssh
  end
```

DHCP addressing mode on an interface

If you configure an interface to use DHCP, the FortiGate unit automatically broadcasts a DHCP request from the interface. The interface is configured with the IP address and any DNS server addresses and default gateway address that the DHCP server provides.

DHCP IPv6 is similar to DHCP IPv4, however there is:

- no default gateway option defined because a host learns the gateway using router advertisement messages
- there is no WINS servers because it is obsolete.

For more information about DHCP IPv6, see RFC 3315.

Configure DHCP for an interface in *System* > *Network* > *Interface* and selecting the interface from the list, and selecting *DHCP* in the *Address Mode*. The table describes the DHCP status information when DHCP is configured for an interface.

Addressing mode section of New Interface page for DHCP information

Status	Displays DHCP status messages as the interface connects to the DHCP server and gets addressing information. Select *Status* to refresh the addressing mode status message. Status can be one of: • **initializing -** No activity. • **connecting -** interface attempts to connect to the DHCP server. • **connected -** interface retrieves an IP address, netmask, and other settings from the DHCP server. • **failed -** interface was unable to retrieve an IP address and other settings from the DHCP server.
Obtained IP/Netmask	The IP address and netmask leased from the DHCP server. Only displayed if *Status* is *connected*.
Renew	Select to renew the DHCP license for this interface. Only displayed if *Status* is *connected*.

Expiry Date	The time and date when the leased IP address and netmask is no longer valid for the interface. The IP address is returned to the pool to be allocated to the next user request for an IP address. Only displayed if *Status* is *connected*.
Default Gateway	The IP address of the gateway defined by the DHCP server. Only displayed if *Status* is *connected*, and if *Receive default gateway from server* is selected.
Distance	Enter the administrative distance for the default gateway retrieved from the DHCP server. The administrative distance, an integer from 1-255, specifies the relative priority of a route when there are multiple routes to the same destination. A lower administrative distance indicates a more preferred route.
Retrieve default gateway from server	Enable to retrieve a default gateway IP address from the DHCP server. The default gateway is added to the static routing table.
Override internal DNS	Enable to use the DNS addresses retrieved from the DHCP server instead of the DNS server IP addresses on the DNS page. When VDOMs are enabled, you can override the internal DNS only on the management VDOM.

PPPoE addressing mode on an interface

If you configure the interface to use PPPoE, the FortiGate unit automatically broadcasts a PPPoE request from the interface.

The FortiGate units support many PPPoE RFC features (RFC 2516) including unnumbered IPs, initial discovery timeout and PPPoE Active Discovery Terminate (PADT).

PPPoE is only configurable in the web-based manager on desktop FortiGate units. 1U FortiGates and up must be configured in the CLI using the commands:

```
config system interface
  edit <port_name>
    set mode pppoe
    set username <ISP_username>
    set password <ISP_password>
    set idle-timeout <seconds>
    set distance <integer>
    set ipunnumbered <unumbered-IP>
    set disc-retry-timeout <seconds>
    set padt-retry-timeout <seconds>
    set lcp-echo-interval <seconds>
    set dns-server-override {enable | disable}
end
```

Configure PPPoE on an interface in *System* > *Network* > *Interface.* The table describes the PPPoE status information when PPPoE is configured for an interface.

Addressing mode section of New Interface page	
Status	Displays PPPoE status messages as the FortiGate unit connects to the PPPoE server and gets addressing information. Select Status to refresh the addressing mode status message. The status is only displayed if you selected *Edit*. Status can be any one of the following 4 messages.
Initializing	No activity.
Connecting	The interface is attempting to connect to the PPPoE server.
Connected	The interface retrieves an IP address, netmask, and other settings from the PPPoE server. When the status is connected, PPPoE connection information is displayed.
Failed	The interface was unable to retrieve an IP address and other information from the PPPoE server.
Reconnect	Select to reconnect to the PPPoE server. Only displayed if Status is connected.
User Name	The PPPoE account user name.
Password	The PPPoE account password.
Unnumbered IP	Specify the IP address for the interface. If your ISP has assigned you a block of IP addresses, use one of them. Otherwise, this IP address can be the same as the IP address of another interface or can be any IP address.
Initial Disc Timeout	Enter Initial discovery timeout. Enter the time to wait before starting to retry a PPPoE discovery.
Initial PADT timeout	Enter Initial PPPoE Active Discovery Terminate (PADT) timeout in seconds. Use this timeout to shut down the PPPoE session if it is idle for this number of seconds. PADT must be supported by your ISP. Set initial PADT timeout to 0 to disable.
Distance	Enter the administrative distance for the default gateway retrieved from the PPPoE server. The administrative distance, an integer from 1-255, specifies the relative priority of a route when there are multiple routes to the same destination. A lower administrative distance indicates a more preferred route. The default distance for the default gateway is 1.
Retrieve default gateway from server	Enable to retrieve a default gateway IP address from a PPPoE server. The default gateway is added to the static routing table.
Override internal DNS	Enable to replace the DNS server IP addresses on the System DNS page with the DNS addresses retrieved from the PPPoE server. When VDOMs are enabled, you can override the internal DNS only on the management VDOM.

Administrative access

Interfaces, especially the public-facing ports can be potentially accessed by those who you may not want access to the FortiGate unit. When setting up the FortiGate unit, you can set the type of protocol an administrator must use to access the FortiGate unit. The options include:

- HTTPS
- HTTP
- SSH
- TELNET
- SNMP
- PING
- FortiManager Access (FMG-Access
- FortiClient Access (FCT-Access)

You can select as many, or as few, even none, that are accessible by an administrator.

This example adds an IPv4 address 172.20.120.100 to the WAN1 interface as well as the administrative access to HTTPS and SSH. As a good practice, set the administrative access when you are setting the IP address for the port.

To add an IP address on the WAN1 interface - web-based manager

1. Go to *System* > *Network* > *Interface*.
2. Select the WAN1 interface row and select *Edit*.
3. Select the *Addressing Mode* of *Manual*.
4. Enter the IP address for the port of 172.20.120.100/24.
5. For *Administrative Access,* select *HTTPS* and *SSH*.
6. Select *OK*.

To create IP address on the WAN1 interface - CLI

```
config system interface
  edit wan1
    set ip 172.20.120.100/24
    set allowaccess https ssh
end
```

When adding to, or removing a protocol, you must type the entire list again. For example, if you have an access list of HTTPS and SSH, and you want to add PING, typing:

```
set allowaccess ping
```

...only PING will be set. In this case, you must type...

```
set allowaccess https ssh ping
```

Wireless

A wireless interface is similar to a physical interface only it does not include a physical connection. The FortiWiFi units enables you to add multiple wireless interfaces that can be available at the same time (the FortiWiFi-30B can only have one wireless interface). On FortiWiFi units, you can configure the device to be either an access point, or a wireless client. As an access point, the FortiWiFi unit can have up to four separate SSIDs, each on their own subnet for wireless access. In client mode, the FortiWiFi only has one SSID, and is used as a receiver, to enable remote users to connect to the existing network using wireless protocols.

Wireless interfaces also require additional security measures to ensure the signal does not get hijacked and data tampered or stolen.

For more information on configuring wireless interfaces see the *Deploying Wireless Networks* Guide.

Interface MTU packet size

You can change the maximum transmission unit (MTU) of the packets that the FortiGate unit transmits to improve network performance. Ideally, the MTU should be the same as the smallest MTU of all the networks between the FortiGate unit and the destination of the packets. If the packets that the FortiGate unit sends are larger than the smallest MTU, they are broken up or fragmented, which slows down transmission. You can easily experiment by lowering the MTU to find an MTU size for optimum network performance.

To change the MTU, select Override default MTU value (1500) and enter the MTU size based on the addressing mode of the interface

- 68 to 1 500 bytes for static mode
- 576 to 1 500 bytes for DHCP mode
- 576 to 1 492 bytes for PPPoE mode
- larger frame sizes if supported by the FortiGate model

Only available on physical interfaces. Virtual interfaces associated with a physical interface inherit the physical interface MTU size.

Interfaces on some models support frames larger than the traditional 1500 bytes. Jumbo frames are supported on FortiGate models that have either a SOC2 or NP4lite, except for the FortiGate-30D, as well as on FortiGate-100D series models (for information about your FortiGate unit's hardware, see the *Hardware Acceleration* guide). For other models, please contact Fortinet Customer Support for the maximum frame size that is supported.

If you need to enable sending larger frames over a route, you need all Ethernet devices on that route to support that larger frame size, otherwise your larger frames will not be recognized and are dropped.

If you have standard size and larger size frame traffic on the same interface, routing alone cannot route them to different routes based only on frame size. However, you can use VLANs to make sure the larger frame traffic is routed over network devices that support that larger size. VLANs will inherit the MTU size from the parent interface. You will need to configure the VLAN to include both ends of the route as well as all switches and routers along the route.

MTU packet size is changed in the CLI. If you select an MTU size larger than your FortiGate unit supports, an error message will indicate this. In this situation, try a smaller MTU size until the value is supported.

In Transparent mode, if you change the MTU of an interface, you must change the MTU of all interfaces on the FortiGate unit to match the new MTU.

To change the MTU size, use the following CLI commands:

```
config system interface
  edit <interface_name>
    set mtu-override enable
    set mtu <byte_size>
end
```

Secondary IP addresses to an interface

If an interface is configured with a manual or static IP address, you can also add secondary static IP addresses to the interface. Adding secondary IP addresses effectively adds multiple IP addresses to the interface. Secondary IP addresses cannot be assigned using DCHP or PPPoE.

All of the IP addresses added to an interface are associated with the single MAC address of the physical interface and all secondary IP addresses are in the same VDOM as the interface that are added to. You configure interface status detection for gateway load balancing separately for each secondary IP addresses. As with all other interface IP addresses, secondary IP addresses cannot be on the same subnet as any other primary or secondary IP address assigned to a FortiGate interface unless they are in separate VDOMs.

To configure a secondary IP, go to *System* > *Network* > *Interface*, select *Edit* or *Create New* and select the *Secondary IP Address* check box.

Virtual domains

Virtual domains (VDOMs) are a method of dividing a FortiGate unit into two or more virtual units that function as multiple independent units. A single FortiGate unit is then flexible enough to serve multiple departments of an organization, separate organizations, or to act as the basis for a service provider's managed security service.

VDOMs provide separate security domains that allow separate zones, user authentication, security policies, routing, and VPN configurations. By default, each FortiGate unit has a VDOM named root. This VDOM includes all of the FortiGate physical interfaces, modem, VLAN subinterfaces, zones, security policies, routing settings, and VPN settings.

When a packet enters a VDOM, it is confined to that VDOM. In a VDOM, you can create security policies for connections between Virtual LAN (VLAN) subinterfaces or zones in the VDOM. Packets do not cross the virtual domain border internally. To travel between VDOMs, a packet must pass through a firewall on a physical interface. The packet then arrives at another VDOM on a different interface, but it must pass through another firewall before entering the VDOM. Both VDOMs are on the same FortiGate unit. Inter-VDOMs change this behavior in that they are internal interfaces; however their packets go through all the same security measures as on physical interfaces.

This example shows how to enable VDOMs on the FortiGate unit and the basic and create a VDOM accounting on the DMZ2 port and assign an administrator to maintain the VDOM. First enable Virtual Domains on the FortiGate unit. When you enable VDOMs, the FortiGate unit will log you out.

For desktop and low-end FortiGate units, VDOMs are enabled using the CLI. On larger FortiGate units, you can enable on the web-based manager or the CLI. Once enabled all further configuration can me made in the web-based manager or CLI.

To enable VDOMs - web-based manager

1. Go to *System* > *Dashboard* > *Status*.

2. In the *System Information* widget, select *Enable* for *Virtual Domain.*

The FortiGate unit logs you out. Once you log back in, you will notice that the menu structure has changed. This reflects the global settings for all Virtual Domains.

To enable VDOMs - CLI

```
config system global
  set vdom-admin enable
end
```

Next, add the VDOM called accounting.

To add a VDOM - web-based manager

1. Go to *System* > *VDOM* > *VDOM*, and select *Create New*.
2. Enter the VDOM name `accounting`.
3. Select *OK*.

To add a VDOM - CLI

```
config vdom
  edit <new_vdom_name>
end
```

With the Virtual Domain created, you can assign a physical interface to it, and assign it an IP address.

To assign physical interface to the accounting Virtual Domain - web-based manager

1. Go to *System* > *Network* > *Interface*.
2. Select the DMZ2 port row and select *Edit*.
3. For the *Virtual Domain* drop-down list, select *accounting*.
4. Select the *Addressing Mode* of *Manual*.
5. Enter the IP address for the port of 10.13.101.100/24.
6. Set the *Administrative Access* to *HTTPS* and *SSH*.
7. Select *OK*.

To assign physical interface to the accounting Virtual Domain - CLI

```
config global
  config system interface
    edit dmz2
      set vdom accounting
      set ip 10.13.101.100/24
      set allowaccess https ssh
  next
end
```

Virtual LANs

The term VLAN subinterface correctly implies the VLAN interface is not a complete interface by itself. You add a VLAN subinterface to the physical interface that receives VLAN-tagged packets. The physical interface can belong to a different VDOM than the VLAN, but it must be connected to a network route that is configured for this VLAN. Without that route, the VLAN will not be connected to the network, and VLAN traffic will not be able to access this interface.The traffic on the VLAN is separate from any other traffic on the physical interface.

FortiGate unit interfaces cannot have overlapping IP addresses, the IP addresses of all interfaces must be on different subnets. This rule applies to both physical interfaces and to virtual interfaces such as VLAN subinterfaces. Each VLAN subinterface must be configured with its own IP address and netmask. This rule helps prevent a broadcast storm or other similar network problems.

Any FortiGate unit, with or without VDOMs enabled, can have a maximum of 255 interfaces in Transparent operating mode. In NAT/Route operating mode, the number can range from 255 to 8192 interfaces per VDOM, depending on the FortiGate model. These numbers include VLANs, other virtual interfaces, and physical interfaces. To have more than 255 interfaces configured in Transparent operating mode, you need to configure multiple VDOMs with many interfaces on each VDOM.

This example shows how to add a VLAN, vlan_accounting on the FortiGate unit internal interface with an IP address of 10.13.101.101.

To add a VLAN - web-based manager

1. Go to *System* > *Network* > *Interface* and select *Create New*.

   The *Type* is by default set to VLAN.
2. Enter a name for the VLAN to `vlan_accounting`.
3. Select the *Internal* interface.
4. Enter the *VLAN ID*.

   The VLAN ID is a number between 1 and 4094 that allow groups of IP addresses with the same VLAN ID to be associated together.
5. Select the *Addressing Mode* of *Manual*.
6. Enter the IP address for the port of 10.13.101.101/24.
7. Set the *Administrative Access* to *HTTPS* and *SSH*.
8. Select *OK*.

To add a VLAN - CLI

```
config system interface
  edit VLAN_1
    set interface internal
    set type vlan
    set vlanid 100
    set ip 10.13.101.101/24
    set allowaccess https ssh
  next
end
```

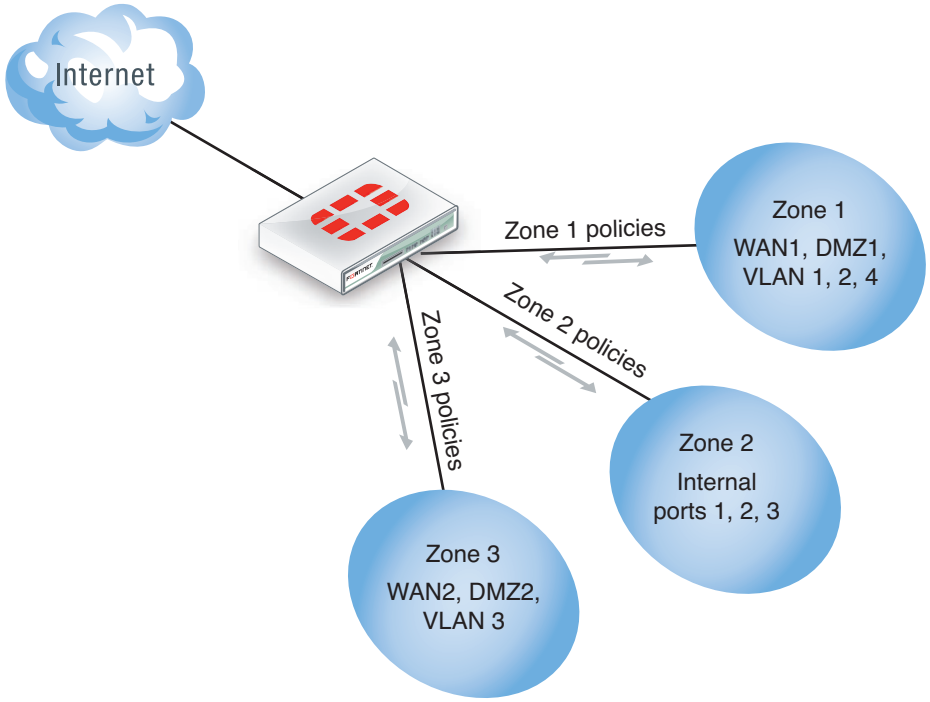
Zones

Zones are a group of one or more FortiGate interfaces, both physical and virtual, that you can apply security policies to control inbound and outbound traffic. Grouping interfaces and VLAN subinterfaces into zones simplifies the creation of security policies where a number of network segments can use the same policy settings and protection profiles. When you add a zone, you select the names of the interfaces and VLAN subinterfaces to add to the zone. Each interface still has its own address and routing is still done between interfaces, that is, routing is not affected by zones. Security policies can also be created to control the flow of intra-zone traffic.

For example, in the illustration below, the network includes three separate groups of users representing different entities on the company network. While each group has its own set of

port and VLANs, in each area, they can all use the same security policy and protection profiles to access the Internet. Rather than the administrator making nine separate security policies, he can add the required interfaces to a zone, and create three policies, making administration simpler.

Figure 16: Network zones



You can configure policies for connections to and from a zone, but not between interfaces in a zone. Using the above example, you can create a security policy to go between zone 1 and zone 3, but not between WAN2 and WAN1, or WAN1 and DMZ1.

This example explains how to set up a zone to include the Internal interface and a VLAN.

To create a zone - web-based manager

1. Go to *System* > *Network* > *Interface.*
2. Select the arrow on the *Create New* button and select *Zone*.
3. Enter a zone name of `Zone_1`.
4. Select the Internal interface and the virtual LAN interface *vlan_accounting* created previously.
5. Select *OK*.

To create a zone - CLI

```
config system zone
  edit Zone_1
    set interface internal VLAN_1
end
```

Probing Interfaces

Server probes can be used on interfaces. In order for this to occur, the probe response must first be enabled and configured, then the probe response must be allowed administrative access on the interface. Both steps must be done through the CLI.

Enabling and configuring the probe

```
config system probe-response
  set http-probe-port <port>
  set http-probe enable
end
```

Allowing the probe response to have administrative access to the interface

```
config system interface
  edit <port>
    set allowaccess  probe-response
  end
end
```

Central management

This chapter describes the basics of using FortiManager as an administration tool for multiple FortiGate units. It describes the basics of setting up a FortiGate unit in FortiManager and some key management features you can use within FortiManager to manage the FortiGate unit.

This section includes the topics:

- Adding a FortiGate to FortiManager
- Configuration through FortiManager
- Firmware updates
- FortiGuard
- Backup and restore configurations
- Administrative domains

In order for the FortiGate unit and FortiManager unit to properly connect, both units must have compatible firmware. To find out if your firmware is compatible, refer to the FortiOS or FortiManager Release Notes.

Adding a FortiGate to FortiManager

Before you can maintain a FortiGate unit using a FortiManager unit, you need to add it to the FortiManager. To do this requires configuration on both the FortiGate and FortiManager. This section describes the basics to configure management using a FortiManager device. For more information on the interaction of FortiManager with the FortiGate unit, see the FortiManager documentation.

FortiGate configuration

These steps ensure that the FortiGate unit will be able to receive updated antivirus and IPS updates and allow remote management through the FortiManager system. You can add a FortiGate unit whether it is running in either NAT mode or transparent mode. The FortiManager unit provides remote management of a FortiGate unit over TCP port 541.

If you have not already done so, register the FortiGate unit by visiting http://support.fortinet.com and select *Product Registration*. By registering your Fortinet unit, you will receive updates to threat detection and prevention databases (Antivirus, Intrusion Detection, etc.) and will also ensure your access to technical support.

You must enable the FortiGate management option so the FortiGate unit can accept management updates to firmware, antivirus signatures, and IPS signatures.

To configure the FortiGate unit - web-based manager

1. Log in to the FortiGate unit.
2. Go to *System* > *Admin* > *Settings*.
3. Enter the *IP address* for the FortiManager unit.
4. Select *Send Request*.

The FortiManager ID now appears in the Trusted FortiManager table.

As an additional security measure, you can also select *Registration Password* and enter a password to connect to the FortiManager.

To configure the FortiGate unit - CLI

```
config system central-mamagement
  set fmg <ip_address>
end
```

To use the registration password enter:

```
execute central-mgmt register-device
    <fmg-serial-no><fmg-register-password><fgt-usrname><fgt-password>
```

Configuring an SSL connection

An SSL connection can be configured between the two devices and an encryption level selected. Use the following CLI commands in the FortiGate CLI to configure the connection:

```
config system central-management
  set status enable
  set enc-algorithm {default* | high | low}
end
```

The default encryption automatically sets high and medium encryption algorithms. Algorithms used for high, medium, and low follows openssl definitions:

- ***High*** - Key lengths larger than 128 bits, and some cipher suites with 128-bit keys.

  Algorithms are: DHE-RSA-AES256-SHA:AES256-SHA: EDH-RSA-DES-CBC3-SHA: DES-CBC3-SHA:DES-CBC3-MD5:DHE-RSA-AES128-SHA:AES128-SHA
- ***Medium*** - Key strengths of 128 bit encryption.

  Algorithms are: RC4-SHA:RC4-MD5:RC4-MD
- ***Low*** - Key strengths of 64 or 56 bit encryption algorithms but excluding export cipher suites

  Algorithms are: EDH-RSA-DES-CDBC-SHA; DES-CBC-SHA; DES-CBC-MD5.

FortiManager configuration

Once the connection between the FortiGate unit and the FortiManager unit has been configured, you can add the FortiGate to the Device Manager in the FortiManager unit's web-based manager.

Configuration through FortiManager

With the FortiManager system, you can monitor and configure multiple FortiGate units from one location and log in. Using the FortiManager's Device Manager, you can view the FortiGate units and make the usual configuration updates and changes, without having to log in and out of multiple FortiGate units.

FortiManager enables you to complete the configuration, by going to the Device Manager, selecting the FortiGate unit and using the same menu structure and pages as you would see in the FortiGate web-based manager. All changes to the FortiGate configuration are stored locally on the FortiManager unit until you synchronize with the FortiGate unit.

When a FortiGate unit is under control of a FortiManager system, administrators will not be able to change the configuration using the FortiGate. When trying to change options, the unit

displays a message that it is configured through FortiManager, and any changes may be reverted.

Global objects

If you are maintaining a number of FortiGate units within a network, many of the policies and configuration elements will be the same across the corporation. In these instances, the adding and editing of many of the same policies will be come a tedious and error-prone activity. With FortiManager global objects, this level of configuration is simplified.

A global object is an object that is not associated specifically with one device or group. Global objects includes security policies, a DNS server, VPN, and IP pools.

The Global Objects window is where you can configure global objects and copy the configurations to the FortiManager device database for a selected device or a group of devices. You can also import configurations from the FortiManager device database for a selected device and modify the configuration as required.

When configuring or creating a global policy object the interface, prompts, and fields are the same as creating the same object on a FortiGate unit using the FortiGate web-based manager.

Locking the FortiGate web-based manager

When you use the FortiManager to manager multiple FortiGate units, a local FortiGate unit becomes locked from any configuration changes using the web-based manager for most administrators. The super_admin will still be able to make changes to the configuration; however, this is not recommended as it may cause conflicts with the FortiManager.

Firmware updates

A FortiManager unit can also perform firmware updates for multiple FortiGate units, saving time rather than upgrading each FortiGate unit individually.

The FortiManager unit stores local copies of firmware images, either by downloading images from the Fortinet Distribution Network (FDN) or by accepting firmware images that are uploaded from the management computer.

If you are using the FortiManager unit to download firmware images, the FDN first validates device licenses and support contracts and then provides a list of currently available firmware images. For devices with valid Fortinet Technical Support contracts, you can download new firmware images from the FDN and the firmware release notes.

After firmware images have been either downloaded from the FDN or imported to the firmware list, you can either schedule or immediately upgrade/downgrade a device or group of device's firmware.

FortiGuard

FortiManager can also connect to the FortiGuard Distribution Network (FDN) to receive push updates for IPS signatures and antivirus definitions. These updates can then be used to update multiple FortiGate units throughout an organization. By using the FortiManager as the host for updates, bandwidth use is minimized as updates are downloaded to one source instead of many.

To receive IPS and antivirus updates from FortiManager, indicate an alternate IP address on the FortiGate unit.

To configure updates from FortiManager

1. Go to *System* > *Config* > *FortiGuard*.
2. Select *AntiVirus and IPS Options* to expand the options.
3. Enable both *Allow Push Update* and *Use override push IP.*
4. Enter the IP address of the FortiManager unit.
5. Select *Apply*.

Backup and restore configurations

FortiManager stores configuration files for backup and restore purposes. FortiManager also enables you to save revisions of configuration files. Configuration backups occur automatically when the administrator logs out, the administrator login session expires, or the FortiGate restarts. Administrators can also start a backup manually.

FortiManager also enables you to view differences between different configurations to view where changes have been made.

Configure the FortiGate as follows to support backing up the configuration to FortiManager:

```
config system central-management
  set mode backup
  set type fortimanager
  set fortimanager-fds-override enable
  set fmg "192.168.206.26"
end
```

On the FortiManager site, the ADOM that includes the FortiGate must be set to backup.

Enabling fortimanager-fds-override means that the FortiGate must use the FortiManager for FortiGuard updates and FortiGuard web filtering lookups.

Administrative domains

FortiManager administrative domains enable the super_admin to create groupings of devices for configured administrators to monitor and manage. FortiManager can manage a large number of Fortinet appliances. This enables administrators to maintain managed devices specific to their geographic location or business division. This also includes FortiGate units with multiple configured VDOMs.

Each administrator is tied to an administrative domain (ADOM). When that particular administrator logs in, they see only those devices or VDOMs configured for that administrator and ADOM. The one exception is the super_admin account that can see and maintain all administrative domains and the devices within those domains.

Administrative domains are not enabled by default and enabling and configuring the domains can only be performed by the super_admin.

The maximum number of administrative domains you can add depends on the FortiManager model.

Monitoring

With network administration, the first step is installing and configuring the FortiGate unit to be the protector of the internal network. Once the system is running efficiently, the next step is to monitor the system and network traffic, making configuration changes as necessary when a threat or vulnerability is discovered.

This chapter discusses the various methods of monitoring both the FortiGate unit and the network traffic through a range of different tools available within FortiOS.

This section includes the topics:

Dashboard

The FortiOS dashboard provides a location to view real-time system information. By default, the dashboard displays the key statistics of the FortiGate unit itself, providing the memory and CPU status, as well as the health of the ports, whether they are up or down and their throughput.

Widgets

Within the dashboard is a number of smaller windows, called widgets, that provide this status information. Beyond what is visible by default, you can add a number of other widgets that display other key traffic information including application use, traffic per IP address, top attacks, traffic history and logging statistics.

You can add multiple dashboards to reflect what data you want to monitor, and add the widgets accordingly. Dashboard configuration is only available through the web-based manager. Administrators must have read and write privileges to customize and add widgets when in either menu. Administrators must have read privileges if they want to view the information.

To add a dashboard and widgets

1. Go to *System* > *Dashboard*.
2. Select the *Dashboard* menu at the top of the window and select *Add Dashboard*.
3. Enter a name for the widget.
4. Select the *Widget* menu at the top of the window.
5. From the screen, select the type of information you want to add.
6. When done, select the X in the top right of the widget.

Dashboard widgets provide an excellent method to view real-time data about the events occurring on the FortiGate unit and the network. For example, by adding the Network Protocol Usage widget, you can monitor the activity of various protocols over a selected span of time. Based on that information you can add or adjust traffic shaping and/or security policies to control traffic.

FortiClient software

The *License Information* widget includes information for the FortiClient connections. It displays the number of FortiClient connections allowed and the number of users connecting. By selecting the *Details* link for the number of connections, you can view more information about the connecting user, including IP address, user name, and type of operating system the user is connecting with.

Included with this information is a link for Mac and Windows. Selecting these links automatically downloads the FortiClient install file (.dmg or .exe) to the management computer.

sFlow

sFlow is a method of monitoring the traffic on your network to identify areas on the network that may impact performance and throughput. FortiOS implements sFlow version 5.

sFlow uses packet sampling to monitor network traffic. The sFlow Agent captures packet information at defined intervals and sends them to an sFlow Collector for analysis, providing real-time data analysis. The information sent is only a sampling of the data for minimal impact on network throughput and performance.

The sFlow Agent is embedded in the FortiGate unit. Once configured, the FortiGate unit sends sFlow datagrams of the sampled traffic to the sFlow Collector, also called an sFlow Analyzer. The sFlow Collector receives the datagrams, and provides real-time analysis and graphing to indicate where potential traffic issues are occurring. sFlow Collector software is available from a number of third party software vendors.

sFlow data captures only a sampling of network traffic, not all traffic like the traffic logs on the FortiGate unit. Sampling works by the sFlow Agent looking at traffic packets when they arrive on an interface. A decision is made whether the packet is dropped and allowed to be to its destination or if a copy is forwarded to the sFlow Collector. The sample used and its frequency are determined during configuration.

sFlow is not supported on virtual interfaces such as vdom link, ipsec, ssl.<vdom> or gre.

The sFlow datagram sent to the Collector contains the information:

- Packet header (e.g. MAC,IPv4,IPv6,IPX,AppleTalk,TCP,UDP, ICMP)
- Sample process parameters (rate, pool etc.)
- Input/output ports
- Priority (802.1p and TOS)
- VLAN (802.1Q)
- Source/destination prefix
- Next hop address
- Source AS, Source Peer AS
- Destination AS Path
- Communities, local preference
- User IDs (TACACS/RADIUS) for source/destination
- URL associated with source/destination
- Interface statistics (RFC 1573, RFC 2233, and RFC 2358)

sFlow agents can be added to any type of FortiGate interface. sFlow isn't supported on some virtual interfaces such as VDOM link, IPsec, gre, and ssl.<vdom>.

For more information on sFlow, Collector software and sFlow MIBs, visit www.sflow.org.

Configuration

sFlow configuration is available only from the CLI. Configuration requires two steps: enabling the sFlow Agent and configuring the interface for the sampling information.

Enable sFlow

```
config system sflow
  set collector-ip <ip_address>
  set collector-port <port_number>
end
```

The default port for sFlow is UDP 6343. To configure in VDOM, use the commands:

```
config system vdom-sflow
  set vdom-sflow enable
  set collector-ip <ip_address>
  set collector-port <port_number>
end
```

Configure sFlow agents per interface.

```
config system interface
  edit <interface_name>
    set sflow-sampler enable
    set sample-rate <every_n_packets>
    set sample-direction [tx | rx | both]
    set polling-interval <seconds>
   end
```

Monitor menus

The *Monitor* menus enable you to view session and policy information and other activity occurring on your FortiGate unit. The monitors provide the details of user activity, traffic and policy usage to show live activity. Monitors are available for DHCP, routing, security policies, traffic shaping, load balancing, security features, VPN, users, WiFi, and logging.

Logging

FortiOS provides a robust logging environment that enables you to monitor, store, and report traffic information and FortiGate events, including attempted log ins and hardware status. Depending on your requirements, you can log to a number of different hosts.

To configure logging in the web-based manager, go to *Log & Report* > *Log Config* > *Log Settings*.

To configure logging in the CLI use the commands `config log <log_location>`.

For details on configuring logging see the *Logging and Reporting Guide.*

If you will be using several FortiGate units, you can also use a FortiAnalyzer unit for logging. For more information, see the *FortiAnalyzer Administration Guide*.

FortiCloud

The FortiCloud is a subscription-based hosted service. With this service, you can have centralized management, logging, and reporting capabilities available in FortiAnalyzer and FortiManager platforms, without any additional hardware to purchase, install or maintain. In most cases, FortiCloud is the recommended location for saving and viewing logs.

This service includes a full range of reporting, analysis and logging, firmware management and configuration revision history. It is hosted within the Fortinet global FortiGuard Network for maximum reliability and performance, and includes reporting, and drill-down analysis widgets makes it easy to develop custom views of network and security events.

The FortiGate unit sends log messages to the FortiCloud using TCP port 443. Configuration is available once a user account has been set up and confirmed. To enable the account on the FortiGate unit, go to *System* > *Dashboard* > *Status*, select *Activate*, and enter the account ID.

For FortiCloud traffic, you can identify a specific port/IP address for logging traffic. Configuration of these services is performed in the CLI, using the command `set source-ip`. When configured, this becomes the dedicated port to send this traffic over.

For example, to set the source IP of the FortiCloud server to be on the DMZ1 port with an IP of 192.168.4.5, the commands are:

```
config log fortiguard setting
  set status enable
  set source-ip 192.168.4.5
end
```

From the FortiGate unit, you can configure the connection and sending of log messages to be sent over an SSL tunnel to ensure log messages are sent securely. To do this, use the CLI commands to enable the encrypted connection and define the level of encryption.

```
config log fortiguard setting
  set status enable
  set enc-alogorithm {default | high | low | disable}
end
```

For more information on each encryption level see “Configuring an SSL connection” on page 139.

FortiGate memory

Logs are saved to the internal memory by default. Inexpensive yet volatile, for basic event logs or verifying traffic, AV or spam patterns, logging to memory is a simple option. However, because logs are stored in the limited space of the internal memory, only a small amount is available for logs. As such logs can fill up and be overridden with new entries, negating the use of recursive data. This is especially true for traffic logs. Also, should the FortiGate unit be shut down or rebooted, all log information will be lost.

FortiGate hard disk

For those FortiGate units with an internal hard disk or SDHC card, you can store logs to this location. Efficient and local, the hard disk provides a convenient storage location. If you choose to store logs in this manner, remember to backup the log data regularly.

Configure log disk settings is performed in the CLI using the commands:

```
config log disk setting
  set status enable
end
```

Further options are available when enabled to configure log file sizes, and uploading/backup events.

As well, note that the write speeds of hard disks compared to the logging of ongoing traffic may cause the dropping such, it is recommended that traffic logging be sent to a FortiAnalyzer or other device meant to handle large volumes of data.

Syslog server

An industry standard for collecting log messages, for off-site storage. In the web-based manager, you are able to send logs to a single syslog server, however in the CLI you can configure up to three syslog servers where you can also use multiple configuration options. For example, send traffic logs to one server, antivirus logs to another. The FortiGate unit sends Syslog traffic over UIDP port 514. Note that if a secure tunnel is configured for communication to a FortiAnalyzer unit, then Syslog traffic will be sent over an IPSec connection, using UPD 500/4500, protocol IP/50.

To configure a Syslog server in the web-based manager, go to *Log & Report* > *Log Config* > *Log Settings*. In the CLI use the commands:

```
config log syslogd setting
  set status enable
end
```

Further options are available when enabled to configure a different port, facility and server IP address.

For Syslog traffic, you can identify a specific port/IP address for logging traffic. Configuration of these services is performed in the CLI, using the command `set source-ip`. When configured, this becomes the dedicated port to send this traffic over.

For example, to set the source IP of a Syslog server to be on the DMZ1 port with an IP of 192.168.4.5, the commands are:

```
config log syslogd setting
  set status enable
  set source-ip 192.168.4.5
end
```

FortiAnalyzer

The FortiAnalyzer family of logging, analyzing, and reporting appliances securely aggregate log data from Fortinet devices and other syslog-compatible devices. Using a comprehensive suite of easily-customized reports, users can filter and review records, including traffic, event, virus, attack, Web content, and email data, mining the data to determine your security stance and assure regulatory compliance. FortiAnalyzer also provides advanced security management functions such as quarantined file archiving, event correlation, vulnerability assessments, traffic analysis, and archiving of email, Web access, instant messaging and file transfer content.

The FortiGate unit sends log messages over UDP port 514 or OFTP (TCP 514). If a secure connection has been configured, log traffic is sent over UDP port 500/4500, Protocol IP/50. For more information on configuring a secure connection see “Sending logs using a secure connection” on page 139.

For FortiAnalyzer traffic, you can identify a specific port/IP address for logging traffic. Configuration of these services is performed in the CLI, using the command set `source-ip`. When configured, this becomes the dedicated port to send this traffic over.

For example, to set the source IP of a FortiAnalyzer unit to be on port 3 with an IP of 192.168.21.12, the commands are:

```
config log fortiguard setting
  set status enable
  set source-ip 192.168.21.12
end
```

Sending logs using a secure connection

From the FortiGate unit, you can configure the connection and sending of log messages over an SSL tunnel to ensure log messages are sent securely. To do this, use the CLI commands below to enable the encrypted connection and define the level of encryption.

You must configure the secure tunnel on ***both*** ends of the tunnel, the FortiGate unit and the FortiAnalyzer unit.

This configuration is for FortiAnalyzer OS version 4.0 MR2 or lower. For version 40 MR3, see "Configuring an SSL connection" on page 139.

To configure a secure connection to the FortiAnalyzer unit

On the FortiAnalyzer unit, enter the commands:

```
config log device
  edit <device_name>
    set secure psk
    set psk <name_of_IPSec_tunnel>
    set id <fortigate_device_name_on_the_fortianalyzer>
end
```

To configure a secure connection on the FortiGate unit

On the FortiGate CLI, enter the commands:

```
config log fortianalyzer setting
  set status enable
  set server <ip_address>
  set local
  set localid <name_of_IPSec_tunnel>
end
```

Configuring an SSL connection

An SSL connection can be configured between the two devices, and an encryption level selected.

Use the CLI commands to configure the encryption connection:

```
config log fortianalyzer setting
  set status enable
  set enc-algorithm {default* | high | low | disable}
end
```

The default encryption automatically sets high and medium encryption algorithms. Algorithms used for high, medium, and low follows openssl definitions:

- ***High*** - Key lengths larger than 128 bits, and some cipher suites with 128-bit keys.

  Algorithms are: DHE-RSA-AES256-SHA:AES256-SHA: EDH-RSA-DES-CBC3-SHA: DES-CBC3-SHA:DES-CBC3-MD5:DHE-RSA-AES128-SHA:AES128-SHA
- ***Medium*** - Key strengths of 128 bit encryption.

  Algorithms are: RC4-SHA:RC4-MD5:RC4-MD
- ***Low*** - Key strengths of 64 or 56 bit encryption algorithms but excluding export cipher suites

  Algorithms are: EDH-RSA-DES-CDBC-SHA; DES-CBC-SHA; DES-CBC-MD5.

If you want to use an IPSec tunnel to connect to the FortiAnalyzer unit, you need to first disable the enc-algorithm:

```
config log fortianalyzer setting
  set status enable
  set enc-algorithm disable
```

Then set the IPSec encryption:

```
set encrypt enable
  set psksecret <preshared_IPSec_tunnel_key>
end
```

Packet Capture

When troubleshooting networks, it helps to look inside the header of the packets. This helps to determine if the packets, route, and destination are all what you expect. Packet capture can also be called a network tap, packet sniffing, or logic analyzing.

To use the packet capture.

1. Go to *System* > *Network* > *Packet Capture*.
2. Select the interface to monitor and select the number of packets to keep.
3. Select *Enable Filters*.
4. Enter the information you want to gather from the packet capture.
5. Select *OK*.

To run the capture, select the play button in the progress column in the packet capture list. If not active, *Not Running* will also appear in the column cell. The progress bar will indicate the status of the capture. You can stop and restart it at any time.

When the capture is complete, select the *Download* icon to save the packet capture file to your hard disk for further analysis.

Packet capture tells you what is happening on the network at a low level. This can be very useful for troubleshooting problems, such as:

- finding missing traffic
- seeing if sessions are setting up properly
- locating ARP problems such as broadcast storm sources and causes
- confirming which address a computer is using on the network if they have multiple addresses or are on multiple networks
- confirming routing is working as you expect
- wireless client connection problems

- intermittent missing PING packets
- a particular type of packet is having problems, such as UDP, which is commonly used for streaming video

If you are running a constant traffic application such as ping, packet capture can tell you if the traffic is reaching the destination, how the port enters and exits the FortiGate unit, if the ARP resolution is correct, and if the traffic is returning to the source as expected. You can also use packet switching to verify that NAT or other configuration is translating addresses or routing traffic the way that you want it to.

Before you start capturing packets, you need to have a good idea of what you are looking for. Capture is used to confirm or deny your ideas about what is happening on the network. If you try capture without a plan to narrow your search, you could end up with too much data to effectively analyze. On the other hand, you need to capture enough packets to really understand all of the patterns and behavior that you are looking for.

Alert email

As an administrator, you want to be certain you can respond quickly to issues occurring on your network or on the FortiGate unit. Alert emails provide an efficient and direct method of notifying an administrator of events. By configuring alert messages, you can define the threshold when a problem becomes critical and needs attention. When this threshold is reached, the FortiGate unit will send an email to one or more individuals, notifying them of the issue.

In the following example, the FortiGate unit is configured to send email to two administrators (admin1 and admin2) when multiple intrusions are detected every two minutes. The FortiGate unit has its own email address on the mail server.

To configure the email service

1. Go to *System* > *Config* > *Messaging Servers*.
2. Complete the following and select *Apply*:

SMTP Server	Enter the address or name of the email server. For example, `smtp.example.com`.
Default Reply To	Enter an email address to associate with the alert email. This field is optional. If you enter an email address here, it overrides the email address entered when configuring alert email in *Log & Report* > *Alert E-mail*.
Authentication	Enable authentication if required by the email server.
SMTP User	FortiGate
Password	**********

To configure alert email - web-based manager

1. Go to *Log & Report* > *Log Config* > *Alert E-mail*.
2. Enter the information:

Email from	fortigate@example.com
Email to	admin1@example.com admin2@example.com

3. For the *Interval Time*, enter `2`.
4. Select *Intrusion Detected*.
5. Select *Apply*.

To configure alert email - CLI

```
config system email-server
  set port 25
  set server smtp.example.com
  set authenticate enable
  set username FortiGate
  set password *************
end
config alertemail setting
  set username fortigate@example.com
  set mailto1 admin1@example.com
  set mailto2 admin2@example.com
  set filter category
  set IPS-logs enable
end
```

SNMP

Simple Network Management Protocol (SNMP) enables you to monitor hardware on your network. You can configure the hardware, such as the FortiGate SNMP agent, to report system information and send traps (alarms or event messages) to SNMP managers. An SNMP manager, or host, is a typically a computer running an application that can read the incoming trap and event messages from the agent and send out SNMP queries to the SNMP agents. A FortiManager unit can act as an SNMP manager to one or more FortiGate units. FortiOS supports SNMP using IPv4 and IPv6 addressing.

By using an SNMP manager, you can access SNMP traps and data from any FortiGate interface or VLAN subinterface configured for SNMP management access. Part of configuring an SNMP manager is to list it as a host in a community on the FortiGate unit it will be monitoring. Otherwise, the SNMP monitor will not receive any traps from that FortiGate unit or be able to query that unit.

The FortiGate SNMP implementation is read-only. SNMP v1, v2c, and v3 compliant SNMP managers have read-only access to FortiGate system information through queries and can receive trap messages from the FortiGate unit.

To monitor FortiGate system information and receive FortiGate traps, you must first compile the Fortinet and FortiGate Management Information Base (MIB) files. A MIB is a text file that describes a list of SNMP data objects that are used by the SNMP manager. These MIBs provide information the SNMP manager needs to interpret the SNMP trap, event, and query messages sent by the FortiGate unit SNMP agent.

FortiGate core MIB files are available for download by going to *System* > *Config* > *SNMP* and selecting the download link on the page.

The Fortinet implementation of SNMP includes support for most of RFC 2665 (Ethernet-like MIB) and most of RFC 1213 (MIB II). For more information, see “Fortinet MIBs” on page 148. RFC support for SNMP v3 includes Architecture for SNMP Frameworks (RFC 3411), and partial support of User-based Security Model (RFC 3414).

SNMP traps alert you to events that occur such as an a full log disk or a virus detected.

SNMP fields contain information about the FortiGate unit, such as CPU usage percentage or the number of sessions. This information is useful for monitoring the condition of the unit on an ongoing basis and to provide more information when a trap occurs.

The FortiGate SNMP v3 implementation includes support for queries, traps, authentication, and privacy. Authentication and encryption are configured in the CLI. See the `system snmp user` command in the *FortiGate CLI Reference*.

SNMP configuration settings

Before a remote SNMP manager can connect to the FortiGate agent, you must configure one or more FortiGate interfaces to accept SNMP connections by going to *System* > *Network* > *Interface*. Select the interface and, in the *Administrative Access*, select *SNMP*.

For VDOMS, SNMP traps can only be sent on interfaces in the management VDOM. Traps cannot be sent over other interfaces outside the management VDOM.

To configure SNMP settings, go to *System* > *Config* > *SNMP.*

SNMP Agent	Select to enable SNMP communication.
Description	Enter descriptive information about the FortiGate unit. The description can be up to 35 characters.
Location	Enter the physical location of the FortiGate unit. The system location description can be up to 35 characters long.
Contact	Enter the contact information for the person responsible for this FortiGate unit. The contact information can be up to 35 characters.
SNMP v1/v2c section To create a new SNMP community, see New SNMP Community page.	
Community Name	The name to identify the community.
Queries	Indicates whether queries protocols (v1 and v2c) are enabled or disabled. A green check mark indicates queries are enabled; a gray x indicates queries are disabled. If one query is disabled and another one enabled, there will still be a green check mark.
Traps	Indicates whether trap protocols (v1 and v2c) are enabled or disabled. A green check mark indicates traps are enabled; a gray x indicates traps are disabled. If one query is disabled and another one enabled, there will still be a green check mark.
Enable	Select the check box to enable or disable the community.
SNMP v3 section To create a new SNMP community, see Create New SNMP V3 User.	
User Name	The name of the SNMPv3 user.
Security Level	The security level of the user.
Notification Host	The IP address or addresses of the host.
Queries	Indicates whether queries are enabled or disabled. A green check mark indicates queries are enabled; a gray x indicates queries are disabled

New SNMP Community page	
Community Name	Enter a name to identify the SNMP community
Hosts (section)	
IP Address	Enter the IP address and Identify the SNMP managers that can use the settings in this SNMP community to monitor the FortiGate unit. You can also set the IP address to 0.0.0.0 to so that any SNMP manager can use this SNMP community.
Interface	Optionally, select the name of the interface that this SNMP manager uses to connect to the FortiGate unit. You only have to select the interface if the SNMP manager is not on the same subnet as the FortiGate unit. This can occur if the SNMP manager is on the Internet or behind a router. In virtual domain mode, the interface must belong to the management VDOM to be able to pass SNMP traps.
Delete	Removes an SNMP manager from the list within the *Hosts* section.
Add	Select to add a blank line to the Hosts list. You can add up to eight SNMP managers to a single community.
Queries (section)	
Protocol	The SNMP protocol. In the v1 row, this means that the settings are for SNMP v1. In the v2c row, this means that the settings are for SNMP v2c.
Port	Enter the port number (161 by default) that the SNMP managers in this community use for SNMP v1 and SNMP v2c queries to receive configuration information from the FortiGate unit. Select the *Enable* check box to activate queries for each SNMP version. **Note:** The SNMP client software and the FortiGate unit must use the same port for queries.
Enable	Select to enable that SNMP protocol.
Traps (section)	
Protocol	The SNMP protocol. In the v1 row, this means that the settings are for SNMP v1. In the v2c row, this means that the settings are for SNMP v2c.
Local	Enter the remote port numbers (port 162 for each by default) that the FortiGate unit uses to send SNMP v1 or SNMP v2c traps to the SNMP managers in this community. Select the *Enable* check box to activate traps for each SNMP version. **Note:** The SNMP client software and the FortiGate unit must use the same port for traps.
Remote	Enter the remote port number (port 162 is default) that the FortiGate unit uses to send SNMP v1 or v2c traps to the SNMP managers in this community. **Note:** The SNMP client software and the FortiGate unit must use the same port for queries.

Enable	Select to activate traps for each SNMP version.
SNMP Event	Enable each SNMP event for which the FortiGate unit should send traps to the SNMP managers in this community. *CPU Over usage* traps sensitivity is slightly reduced, by spreading values out over 8 polling cycles. This prevents sharp spikes due to CPU intensive short-term events such as changing a policy. *Power Supply Failure* event trap is available only on some models. *AMC interfaces enter bypass mode* event trap is available only on models that support AMC modules.
Enable	Select to enable the SNMP event.
Create New SNMP V3 User	
User Name	Enter the name of the user.
Security Level	Select the type of security level the user will have.
Notification Host	Enter the IP address of the notification host. If you want to add more than one host, after entering the IP address of the first host, select the plus sign to add another host.
Enable Query	Select to enable or disable the query. By default, the query is enabled.
Port	Enter the port number in the field.
Events	Select the SNMP events that will be associated with that user.

Gigabit interfaces

When determining the interface speed of a FortiGate unit with a 10G interface, the IF-MIB.ifSpeed may not return the correct value. IF-MIB.ifSpeed is a 32-bit gauge used to report interface speeds in bits/second and cannot convert to a 64-bit value. The 32-bit counter wrap the output too fast to be accurate.

In this case, you can use the value ifHighSpeed. It reports interface speeds in megabits/second. This ensures that 10Gb interfaces report the correct value.

SNMP agent

You need to first enter information and enable the FortiGate SNMP Agent. Enter information about the FortiGate unit to identify it so that when your SNMP manager receives traps from the FortiGate unit, you will know which unit sent the information.

To configure the SNMP agent - web-based manager

1. Go to *System* > *Config* > *SNMP*.
2. Select *Enable* for the *SNMP Agent*.
3. Enter a descriptive name for the agent.
4. Enter the location of the FortiGate unit.
5. Enter a contact or administrator for the SNMP Agent or FortiGate unit.
6. Select *Apply*.

To configure SNMP agent - CLI

```
config system snmp sysinfo
  set status enable
  set contact-info <contact_information>
  set description <description_of_FortiGate>
  set location <FortiGate_location>
end
```

SNMP community

An SNMP community is a grouping of devices for network administration purposes. Within that SNMP community, devices can communicate by sending and receiving traps and other information. One device can belong to multiple communities, such as one administrator terminal monitoring both a firewall SNMP and a printer SNMP community.

Add SNMP communities to your FortiGate unit so that SNMP managers can connect to view system information and receive SNMP traps.

You can add up to three SNMP communities. Each community can have a different configuration for SNMP queries and traps. Each community can be configured to monitor the FortiGate unit for a different set of events. You can also add the IP addresses of up to 8 SNMP managers to each community.

When the FortiGate unit is in virtual domain mode, SNMP traps can only be sent on interfaces in the management virtual domain. Traps cannot be sent over other interfaces.

To add an SNMP v1/v2c community - web-based manager

1. Go to *System* > *Config* > *SNMP.*
2. In the *SNMP v1/v2c* area, select *Create New*.
3. Enter a *Community Name*.
4. Enter the IP address and Identify the SNMP managers that can use the settings in this SNMP community to monitor the FortiGate unit.
5. Select the interface if the SNMP manager is not on the same subnet as the FortiGate unit.
6. Enter the *Port* number that the SNMP managers in this community use for SNMP v1 and SNMP v2c queries to receive configuration information from the FortiGate unit. Select the *Enable* check box to activate queries for each SNMP version.
7. Enter the Local and Remote port numbers that the FortiGate unit uses to send SNMP v1 and SNMP v2c traps to the SNMP managers in this community.
8. Select the *Enable* check box to activate traps for each SNMP version.
9. Select *OK*.

To add an SNMP v1/v2c community - CLI

```
config system snmp community
  edit <index_number>
    set events <events_list>
    set name <community_name>
    set query-v1-port <port_number>
    set query-v1-status {enable | disable}
    set query-v2c-port <port_number>
    set query-v2c-status {enable | disable}
    set status {enable | disable}
    set trap-v1-lport <port_number>
    set trap-v1-rport <port_number>
    set trap-v1-status {enable | disable}
    set trap-v2c-lport <port_number>
    set trap-v2c-rport <port_number>
    set trap-v2c-status {enable | disable}
end
```

To add an SNMP v3 community - web-based manager

1. Go to *System* > *Config* > *SNMP.*
2. In the *SNMP v3* area, select *Create New*.
3. Enter a *User Name*.
4. Select a *Security Level* and associated authorization algorithms.
5. Enter the IP address of the *Notification Host* SNMP managers that can use the settings in this SNMP community to monitor the FortiGate unit.
6. Enter the *Port* number that the SNMP managers in this community use to receive configuration information from the FortiGate unit. Select the *Enable* check box to activate queries for each SNMP version.
7. Select the *Enable* check box to activate traps.
8. Select *OK*.

To add an SNMP v3 community - CLI

```
config system snmp user
  edit <index_number>
    set security-level [auth-priv | auth-no-priv | no-auth-no-priv}
    set queries enable
    set query-port <port_number>
    set notify-hosts <ip_address>
    set events <event_selections>
end
```

Enabling on the interface

Before a remote SNMP manager can connect to the FortiGate agent, you must configure one or more FortiGate interfaces to accept SNMP connections.

To configure SNMP access - web-based manager

1. Go to *System* > *Network* > *Interface*.
2. Choose an interface that an SNMP manager connects to and select *Edit*.

3. In *Administrative Access*, select *SNMP*.
4. Select *OK*.

To configure SNMP access - CLI

```
config system interface
  edit <interface_name>
    set allowaccess snmp
end
```

If the interface you are configuring already has protocols that are allowed access, use the command `append allowaccess snmp` instead, or else the other protocols will be replaced. For more information, see "Adding and removing options from lists" on page 45.

Fortinet MIBs

The FortiGate SNMP agent supports Fortinet proprietary MIBs as well as standard RFC 1213 and RFC 2665 MIBs. RFC support includes support for the parts of RFC 2665 (Ethernet-like MIB) and the parts of RFC 1213 (MIB II) that apply to FortiGate unit configuration.

There are two MIB files for FortiGate units - the Fortinet MIB, and the FortiGate MIB. The Fortinet MIB contains traps, fields and information that is common to all Fortinet products. The FortiGate MIB contains traps, fields and information that is specific to FortiGate units. Each Fortinet product has its own MIB. If you use other Fortinet products you will need to download their MIB files as well. Both MIB files are used for FortiOS and FortiOS Carrier; there are no additional traps for the Carrier version of the operating system.

The Fortinet MIB and FortiGate MIB along with the two RFC MIBs are listed in tables in this section. You can download the two FortiGate MIB files from Fortinet Customer Support. The Fortinet MIB contains information for Fortinet products in general. the Fortinet FortiGate MIB includes the system information for The FortiGate unit and version of FortiOS. Both files are required for proper SNMP data collection.

To download the MIB files, go to *System* > *Config* > *SNMP* and select a MIB link in the *FortiGate SNMP MIB* section.

Your SNMP manager may already include standard and private MIBs in a compiled database that is ready to use. You must add the Fortinet proprietary MIB to this database to have access to the Fortinet specific information.

There were major changes to the MIB files between v3.0 and v4.0. You need to use the new MIBs for v4.0 or you may mistakenly access the wrong traps and fields.

MIB files are updated for each version of FortiOS. When upgrading the firmware ensure that you updated the Fortinet FortiGate MIB file as well.

Table 9: Fortinet MIBs

MIB file name or RFC	Description
FORTINET-CORE-MIB.mib	The Fortinet MIB includes all system configuration information and trap information that is common to all Fortinet products. Your SNMP manager requires this information to monitor FortiGate unit configuration settings and receive traps from the FortiGate SNMP agent.
FORTINET-FORTIGATE-MIB.mib	The FortiGate MIB includes all system configuration information and trap information that is specific to FortiGate units. Your SNMP manager requires this information to monitor FortiGate configuration settings and receive traps from the FortiGate SNMP agent. FortiManager systems require this MIB to monitor FortiGate units.
RFC-1213 (MIB II)	The FortiGate SNMP agent supports MIB II groups with these exceptions. • No support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10). • Protocol statistics returned for MIB II groups (IP/ICMP/TCP/UDP/etc.) do not accurately capture all FortiGate traffic activity. More accurate information can be obtained from the information reported by the Fortinet MIB.
RFC-2665 (Ethernet-like MIB)	The FortiGate SNMP agent supports Ethernet-like MIB information. FortiGate SNMP does not support for the dot3Tests and dot3Errors groups.

SNMP get command syntax

Normally, to get configuration and status information for a FortiGate unit, an SNMP manager would use an SNMP get commands to get the information in a MIB field. The SNMP get command syntax would be similar to:

```
snmpget -v2c -c <community_name> <address_ipv4> {<OID> | <MIB_field>}
```

…where…

`<community_name>` is an SNMP community name added to the FortiGate configuration. You can add more than one community name to a FortiGate SNMP configuration. The most commonly used community name is `public`.

`<address_ipv4>` is the IP address of the FortiGate interface that the SNMP manager connects to.

`{<OID> | <MIB_field>}` is the object identifier (OID) for the MIB field or the MIB field name itself.

The SNMP `get` command gets firmware version running on the FortiGate unit. The community name is `public`. The IP address of the interface configured for SNMP management access is `10.10.10.1`. The firmware version MIB field is `fgSysVersion` and the OID for this MIB field is

`1.3.6.1.4.1.12356.101.4.1.1` The first command uses the MIB field name and the second uses the OID:

```
snmpget -v2c -c public 10.10.10.1 fgSysVersion.0
snmpget -v2c -c public 10.10.10.1 1.3.6.1.4.1.12356.101.4.1.1.0
```

The OIDs and object names used in these examples are dependent on the version of MIB and are subject to change.

VLANs

Virtual Local Area Networks (VLANs) multiply the capabilities of your FortiGate unit, and can also provide added network security. Virtual LANs (VLANs) use ID tags to logically separate devices on a network into smaller broadcast domains. These smaller domains forward packets only to devices that are part of that VLAN domain. This reduces traffic and increases network security.

A Local Area Network (LAN) is a group of connected computers and devices that are arranged into network broadcast domains. A LAN broadcast domain includes all the computers that receive a packet broadcast from any computer in that broadcast domain. A switch will automatically forward the packets to all of its ports; in contrast, routers do not automatically forward network broadcast packets. This means routers separate broadcast domains. If a network has only switches and no routers, that network is considered one broadcast domain, no matter how large or small it is. Smaller broadcast domains are more efficient because fewer devices receive unnecessary packets. They are more secure as well because a hacker reading traffic on the network will have access to only a small portion of the network instead of the entire network's traffic.

Virtual LANs (VLANs) use ID tags to logically separate a LAN into smaller broadcast domains. Each VLAN is its own broadcast domain. Smaller broadcast domains reduce traffic and increase network security. The IEEE 802.1Q standard defines VLANs. All layer-2 and layer-3 devices along a route must be 802.1Q-compliant to support VLANs along that route. For more information, see "VLAN switching and routing" on page 152 and "VLAN layer-3 routing" on page 155.

VLANs reduce the size of the broadcast domains by only forwarding packets to interfaces that are part of that VLAN or part of a VLAN trunk link. Trunk links form switch-to-switch or switch-to-router connections, and forward traffic for all VLANs. This enables a VLAN to include devices that are part of the same broadcast domain, but physically distant from each other.

VLAN ID tags consist of a 4-byte frame extension that switches and routers apply to every packet sent and received in the VLAN. Workstations and desktop computers, which are commonly originators or destinations of network traffic, are not an active part of the VLAN process. All the VLAN tagging and tag removal is done after the packet has left the computer. For more information, see "VLAN ID rules" on page 152.

Any FortiGate unit without VDOMs enabled can have a maximum of 255 interfaces in transparent operating mode. The same is true for any single VDOM. In NAT mode, the number can range from 255 to 8192 interfaces per VDOM, depending on the FortiGate model. These numbers include VLANs, other virtual interfaces, and physical interfaces. To have more than 255 interfaces configured in transparent operating mode, you need to configure multiple VDOMs that enable you to divide the total number of interfaces over all the VDOMs.

One example of an application of VLANs is a company's accounting department. Accounting computers may be located at both main and branch offices. However, accounting computers need to communicate with each other frequently and require increased security. VLANs allow the accounting network traffic to be sent only to accounting computers and to connect accounting computers in different locations as if they were on the same physical subnet.

This guide uses the term "packet" to refer to both layer-2 frames and layer-3 packets.

VLAN ID rules

Layer-2 switches and layer-3 devices add VLAN ID tags to the traffic as it arrives and remove them before they deliver the traffic to its final destination. Devices such as PCs and servers on the network do not require any special configuration for VLANs. Twelve bits of the 4-byte VLAN tag are reserved for the VLAN ID number. Valid VLAN ID numbers are from 1 to 4094, while 0 is used for high priority frames, and 4095 is reserved.

On a layer-2 switch, you can have only one VLAN subinterface per physical interface, unless that interface is configured as a trunk link. Trunk links can transport traffic for multiple VLANs to other parts of the network.

On a FortiGate unit, you can add multiple VLANs to the same physical interface. However, VLAN subinterfaces added to the same physical interface cannot have the same VLAN ID or have IP addresses on the same subnet. You can add VLAN subinterfaces with the same VLAN ID to different physical interfaces.

Creating VLAN subinterfaces with the same VLAN ID does not create any internal connection between them. For example a VLAN ID of 300 on port1 and VLAN ID of 300 on port2 are allowed, but they are not connected. Their relationship is the same as between any two FortiGate network interfaces.

VLAN switching and routing

VLAN switching takes place on the OSI model layer-2, just like other network switching. VLAN routing takes place on the OSI model layer-3. The difference between them is that during VLAN switching, VLAN packets are simply forwarded to their destination. This is different from VLAN routing where devices can open the VLAN packets and change their VLAN ID tags to route the packets to a new destination.

VLAN layer-2 switching

Ethernet switches are layer-2 devices, and generally are 802.1Q compliant. Layer 2 refers to the second layer of the seven layer Open Systems Interconnect (OSI) basic networking model; the Data Link layer. FortiGate units act as layer-2 switches or bridges when they are in transparent mode. The units simply tag and forward the VLAN traffic or receive and remove the tags from the packets. A layer-2 device does not inspect incoming packets or change their contents; it only adds or removes tags and routes the packet.

A VLAN can have any number of physical interfaces assigned to it. Multiple VLANs can be assigned to the same physical interface. Typically two or more physical interfaces are assigned to a VLAN, one for incoming and one for outgoing traffic. Multiple VLANs can be configured on one FortiGate unit, including trunk links.

Layer-2 VLAN example

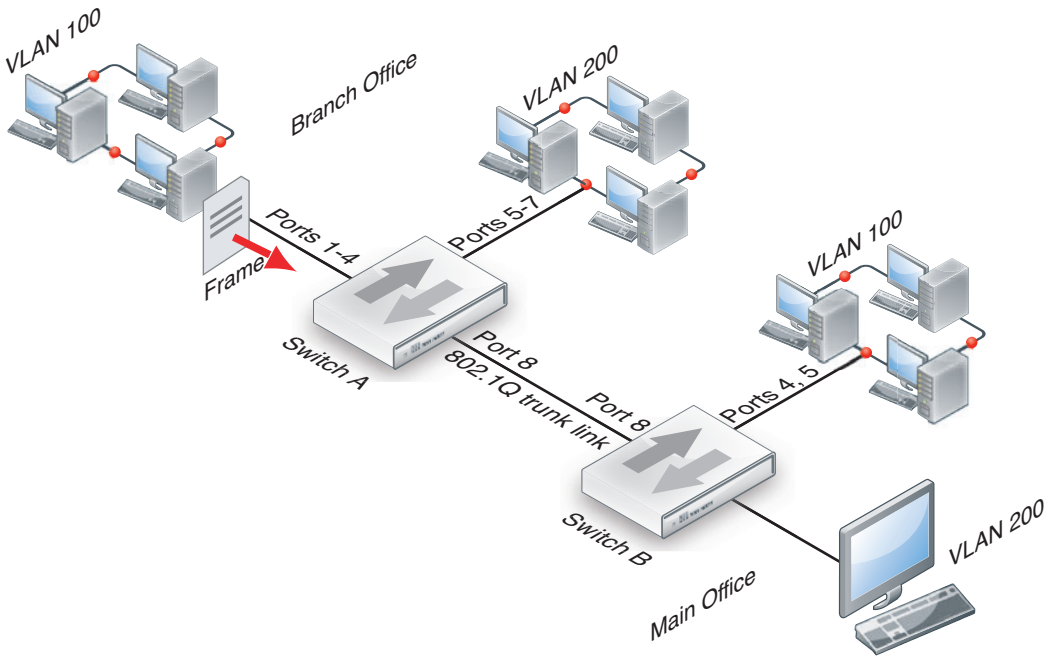
To better understand VLAN operation, this example shows what happens to a data frame on a network that uses VLANs.

The network topology consists of two 8-port switches that are configured to support VLANs on a network. Both switches are connected through port 8 using an 802.1Q trunk link. Subnet 1 is connected to switch A, and subnet 2 is connected to switch B. The ports on the switches are configured as follows.

Table 10: How ports and VLANs are used on Switch A and B

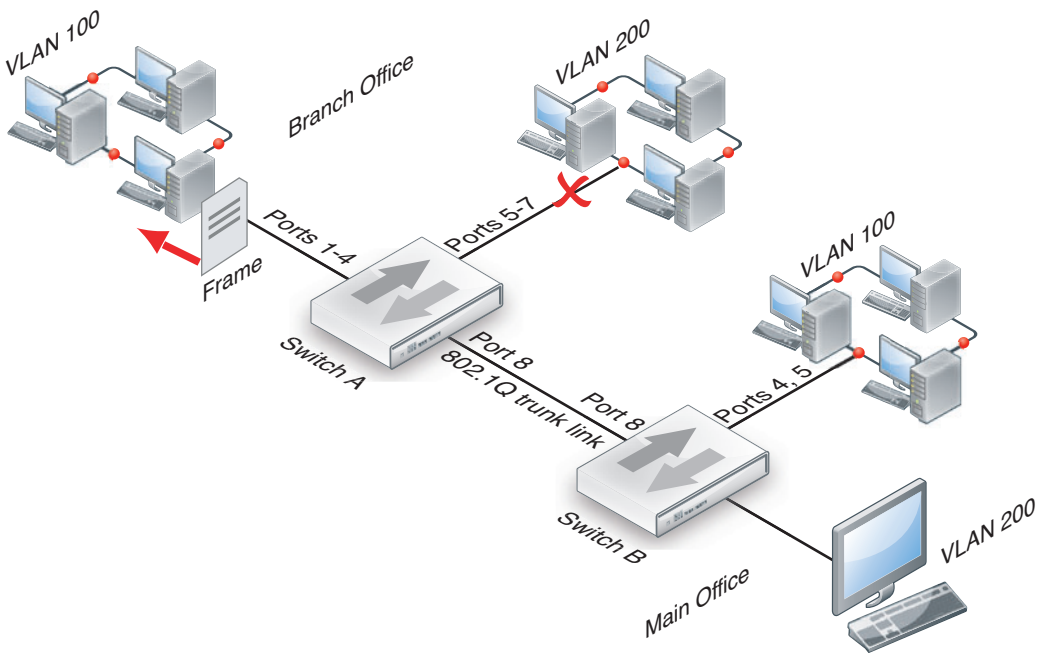
Switch	Ports	VLAN
A	1 - 4	100
A	5 - 7	200
A & B	8	Trunk link
B	4 - 5	100
B	6	200

In this example, switch A is connected to the Branch Office and switch B to the Main Office.



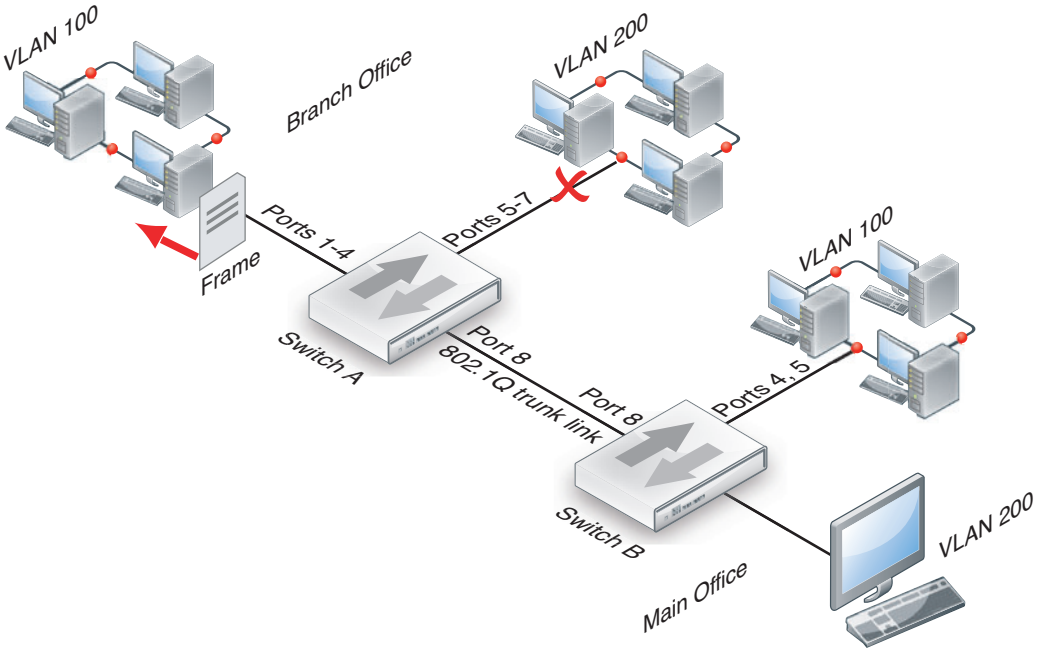
1. A computer on port 1 of switch A sends a data frame over the network.
2. Switch A tags the data frame with a VLAN 100 ID tag upon arrival because port 1 is part of VLAN 100.
3. Switch A forwards the tagged data frame to the other VLAN 100 ports — ports 2 through 4. Switch A also forwards the data frame to the 802.1Q trunk link (port 8) so other parts of the network that may contain VLAN 100 groups will receive VLAN 100 traffic.

This data frame is not forwarded to the other ports on switch A because they are not part of VLAN 100. This increases security and decreases network traffic.



4. Switch B receives the data frame over the trunk link (port 8).
5. Because there are VLAN 100 ports on switch B (ports 4 and 5), the data frame is forwarded to those ports. As with switch A, the data frame is not delivered to VLAN 200.

   If there were no VLAN 100 ports on switch B, the switch would not forward the data frame and it would stop there.



6. The switch removes the VLAN 100 ID tag before it forwards the data frame to an end destination.

The sending and receiving computers are not aware of any VLAN tagging on the data frames that are being transmitted. When any computer receives that data frame, it appears as a normal data frame.

VLAN layer-3 routing

Routers are layer-3 devices. Layer 3 refers to the third layer of the OSI networking model, the Network layer. FortiGate units in NAT mode act as layer-3 devices. As with layer 2, FortiGate units acting as layer-3 devices are 802.1Q-compliant.

The main difference between layer-2 and layer-3 devices is how they process VLAN tags. Layer-2 switches just add, read and remove the tags. They do not alter the tags or do any other high-level actions. Layer-3 routers not only add, read and remove tags but also analyze the data frame and its contents. This analysis allows layer-3 routers to change the VLAN tag if it is appropriate and send the data frame out on a different VLAN.

In a layer-3 environment, the 802.1Q-compliant router receives the data frame and assigns a VLAN ID. The router then forwards the data frame to other members of the same VLAN broadcast domain. The broadcast domain can include local ports, layer-2 devices and layer-3 devices such as routers and firewalls. When a layer-3 device receives the data frame, the device removes the VLAN tag and examines its contents to decide what to do with the data frame. The layer-3 device considers:

- source and destination addresses
- protocol
- port number.

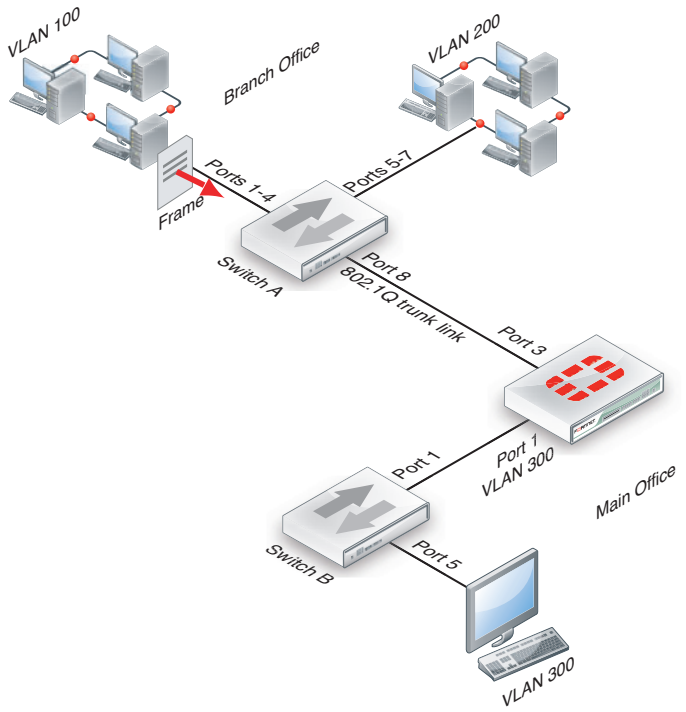
The data frame may be forwarded to another VLAN, sent to a regular non-VLAN-tagged network or just forwarded to the same VLAN as a layer-2 switch would do. Or, the data frame may be discarded if the proper security policy has been configured to do so.

Layer-3 VLAN example

In this example, switch A is connected to the Branch Office subnet, the same as subnet 1 in the layer-2 example. In the Main Office subnet, VLAN 300 is on port 5 of switch B. The FortiGate unit is connected to switch B on port 1 and the trunk link connects the FortiGate unit's port 3 to switch A. The other ports on switch B are unassigned.

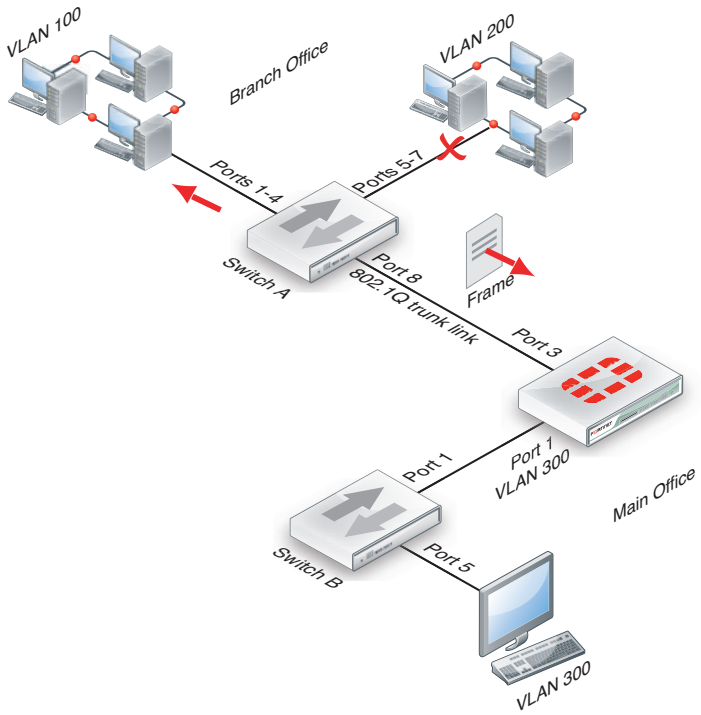
This example explains how traffic can change VLANs originating on VLAN 100 and arriving at a destination on VLAN 300. Layer-2 switches alone cannot accomplish this, but a layer-3 router can.

1. The VLAN 100 computer at the Branch Office sends the data frame to switch A, where the VLAN 100 tag is added.



2. Switch A forwards the tagged data frame to the FortiGate unit over the 802.1Q trunk link, and to the VLAN 100 interfaces on Switch A.

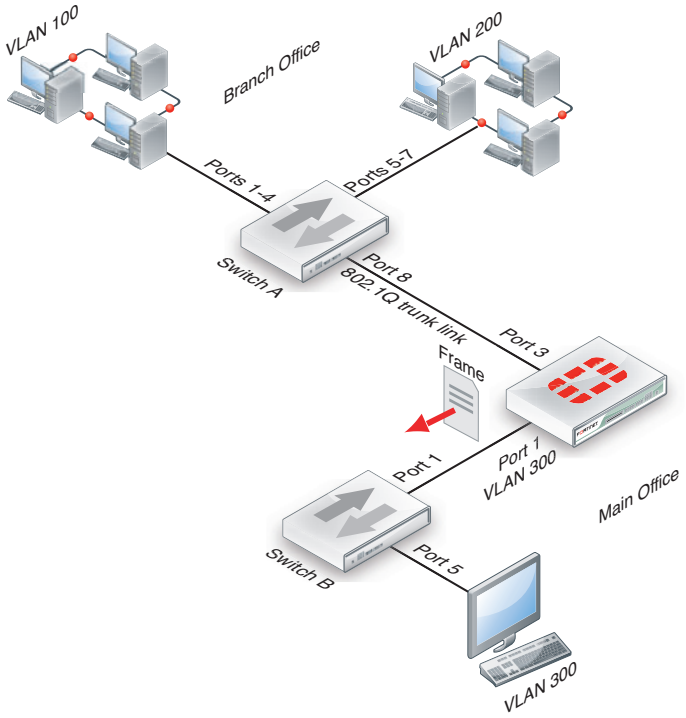
   Up to this point everything is the same as in the layer-2 example.



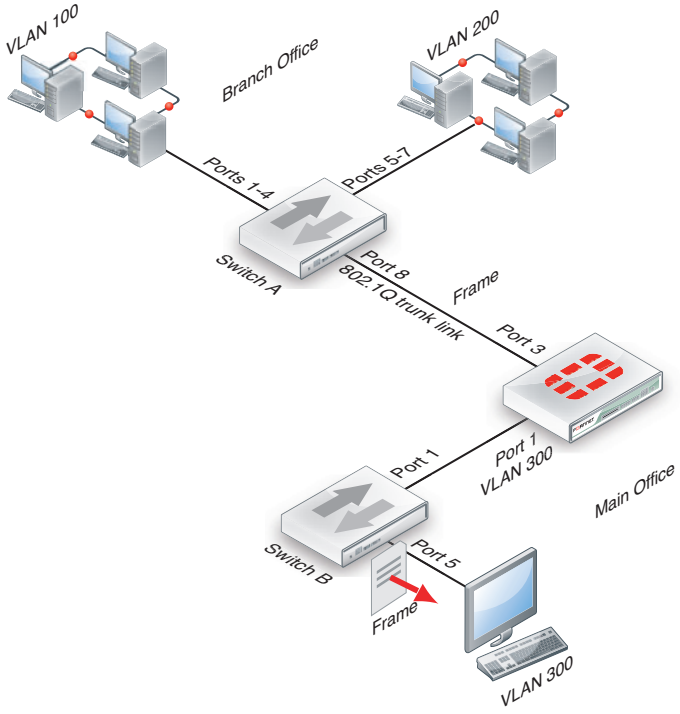
3. The FortiGate unit removes the VLAN 100 tag, and inspects the content of the data frame. The FortiGate unit uses the content to select the correct security policy and routing options.
4. The FortiGate unit's security policy allows the data frame to go to VLAN 300 in this example. The data frame will be sent to all VLAN 300 interfaces, but in the example there is only port 1

on the FortiGate unit. Before the data frame leaves, the FortiGate unit adds the VLAN ID 300 tag to the data frame.

This is the step that layer 2 cannot do. Only layer 3 can retag a data frame as a different VLAN.



5. Switch B receives the data frame, and removes the VLAN ID 300 tag, because this is the last hop, and forwards the data frame to the computer on port 5.



In this example, a data frame arrived at the FortiGate unit tagged as VLAN 100. After checking its content, the FortiGate unit retagged the data frame for VLAN 300. It is this change from

VLAN 100 to VLAN 300 that requires a layer-3 routing device, in this case the FortiGate unit. Layer-2 switches cannot perform this change.

VLANs in NAT mode

In NAT mode the FortiGate unit functions as a layer-3 device. In this mode, the FortiGate unit controls the flow of packets between VLANs, but can also remove VLAN tags from incoming VLAN packets. The FortiGate unit can also forward untagged packets to other networks, such as the Internet.

In NAT mode, the FortiGate unit supports VLAN trunk links with IEEE 802.1Q-compliant switches, or routers. The trunk link transports VLAN-tagged packets between physical subnets or networks. When you add VLAN sub-interfaces to the FortiGate unit physical interfaces, the VLANs have IDs that match the VLAN IDs of packets on the trunk link. The FortiGate unit directs packets with VLAN IDs to sub-interfaces with matching IDs.

You can define VLAN sub-interfaces on all FortiGate physical interfaces. However, if multiple virtual domains are configured on the FortiGate unit, you will have access to only the physical interfaces on your virtual domain. The FortiGate unit can tag packets leaving on a VLAN subinterface. It can also remove VLAN tags from incoming packets and add a different VLAN tag to outgoing packets.

Normally in VLAN configurations, the FortiGate unit's internal interface is connected to a VLAN trunk, and the external interface connects to an Internet router that is not configured for VLANs. In this configuration the FortiGate unit can apply different policies for traffic on each VLAN interface connected to the internal interface, which results in less network traffic and better security.

Adding VLAN subinterfaces

A VLAN subinterface, also called a VLAN, is a virtual interface on a physical interface. The subinterface allows routing of VLAN tagged packets using that physical interface, but it is separate from any other traffic on the physical interface.

Adding a VLAN subinterface includes configuring:

- Physical interface
- IP address and netmask
- VLAN ID
- VDOM

Physical interface

The term VLAN subinterface correctly implies the VLAN interface is not a complete interface by itself. You add a VLAN subinterface to the physical interface that receives VLAN-tagged packets. The physical interface can belong to a different VDOM than the VLAN, but it must be connected to a network router that is configured for this VLAN. Without that router, the VLAN will not be connected to the network, and VLAN traffic will not be able to access this interface. The traffic on the VLAN is separate from any other traffic on the physical interface.

When you are working with interfaces on your FortiGate unit, use the *Column Settings* on the Interface display to make sure the information you need is displayed. When working with VLANs, it is useful to position the *VLAN ID* column close to the IP address. If you are working with VDOMs, including the *Virtual Domain* column as well will help you troubleshoot problems more quickly.

To view the Interface display, go to *System* > *Network* > *Interface*.

IP address and netmask

FortiGate unit interfaces cannot have overlapping IP addresses. The IP addresses of all interfaces must be on different subnets. This rule applies to both physical interfaces and to virtual interfaces such as VLAN subinterfaces. Each VLAN subinterface must be configured with its own IP address and netmask pair. This rule helps prevent a broadcast storm or other similar network problems.

If you are unable to change your existing configurations to prevent IP overlap, enter the CLI command `config system global` and `set ip-overlap enable` to allow IP address overlap. If you enter this command, multiple VLAN interfaces can have an IP address that is part of a subnet used by another interface. This command is recommended for advanced users only.

VLAN ID

The VLAN ID is part of the VLAN tag added to the packets by VLAN switches and routers. The VLAN ID is a number between 1 and 4094 that allow groups of IP addresses with the same VLAN ID to be associated together. VLAN ID 0 is used only for high priority frames, and 4095 is reserved.

All devices along a route must support the VLAN ID of the traffic along that route. Otherwise, the traffic will be discarded before reaching its destination. For example, if your computer is part of VLAN_100 and a co-worker on a different floor of your building is also on the same VLAN_100, you can communicate with each other over VLAN_100, only if all the switches and routers support VLANs and are configured to pass along VLAN_100 traffic properly. Otherwise, any traffic you send your co-worker will be blocked or not delivered.

VDOM

If VDOMs are enabled, each VLAN subinterface must belong to a VDOM. This rule also applies for physical interfaces.

Interface-related CLI commands require a VDOM to be specified, regardless of whether the FortiGate unit has VDOMs enabled.

VLAN subinterfaces on separate VDOMs cannot communicate directly with each other. In this situation, the VLAN traffic must exit the FortiGate unit and re-enter the unit again, passing through firewalls in both directions. This situation is the same for physical interfaces.

A VLAN subinterface can belong to a different VDOM than the physical interface it is part of. This is because the traffic on the VLAN is handled separately from the other traffic on that interface. This is one of the main strengths of VLANs.

The following procedure will add a VLAN subinterface called `VLAN_100` to the FortiGate internal interface with a VLAN ID of 100. It will have an IP address and netmask of `172.100.1.1/255.255.255.0`, and allow HTTPS, PING, and Telnet administrative access. Note that in the CLI, you must enter "`set type vlan`" before setting the vlanid, and that the allowaccess protocols are lower case.

To add a VLAN subinterface in NAT mode - web-based manager

1. If *Current VDOM* appears at the bottom left of the screen, select *Global* from the list of VDOMs.
2. Go to *System* > *Network* > *Interface*.

3. Select *Create New* to add a VLAN subinterface.
4. Enter the following:

VLAN Name	VLAN_100
Type	VLAN
Interface	internal
VLAN ID	100
Addressing Mod	Manual
IP/Netmask	172.100.1.1/255.255.255.0
Administrative Access	HTTPS, PING, TELNET

5. Select *OK*.

To view the new VLAN subinterface, select the expand arrow next to the parent physical interface (the internal interface). This will expand the display to show all VLAN subinterfaces on this physical interface. If there is no expand arrow displayed, there are no subinterfaces configured on that physical interface.

For each VLAN, the list displays the name of the VLAN, and, depending on column settings, its IP address, the Administrative access you selected for it, the VLAN ID number, and which VDOM it belongs to if VDOMs are enabled.

To add a VLAN subinterface in NAT mode - CLI

```
config system interface
  edit VLAN_100
    set interface internal
    set type vlan
    set vlanid 100
    set ip 172.100.1.1 255.255.255.0
    set allowaccess https ping telnet
end
```

Configuring security policies and routing

Once you have created a VLAN subinterface on the FortiGate unit, you need to configure security policies and routing for that VLAN. Without these, the FortiGate unit will not pass VLAN traffic to its intended destination. Security policies direct traffic through the FortiGate unit between interfaces. Routing directs traffic across the network.

Configuring security policies

Security policies permit communication between the FortiGate unit's network interfaces based on source and destination IP addresses. Interfaces that communicate with the VLAN interface need security policies to permit traffic to pass between them and the VLAN interface.

Each VLAN needs a security policy for each of the following connections the VLAN will be using:

- from this VLAN to an external network
- from an external network to this VLAN
- from this VLAN to another VLAN in the same virtual domain on the FortiGate unit
- from another VLAN to this VLAN in the same virtual domain on the FortiGate unit.

The packets on each VLAN are subject to antivirus scans and other UTM measures as they pass through the FortiGate unit.

Configuring routing

As a minimum, you need to configure a default static route to a gateway with access to an external network for outbound packets. In more complex cases, you will have to configure different static or dynamic routes based on packet source and destination addresses.

As with firewalls, you need to configure routes for VLAN traffic. VLANs need routing and a gateway configured to send and receive packets outside their local subnet just as physical interfaces do. The type of routing you configure, static or dynamic, will depend on the routing used by the subnet and interfaces you are connecting to. Dynamic routing can be routing information protocol (RIP), border gateway protocol (BGP), open shortest path first (OSPF), or multicast.

If you enable SSH, PING, Telnet, HTTPS and HTTP on the VLAN, you can use those protocols to troubleshoot your routing and test that it is properly configured. Enabling logging on the interfaces and using CLI diagnose commands such as `diagnose sniff packet <interface_name>` can also help locate any possible configuration or hardware issues.

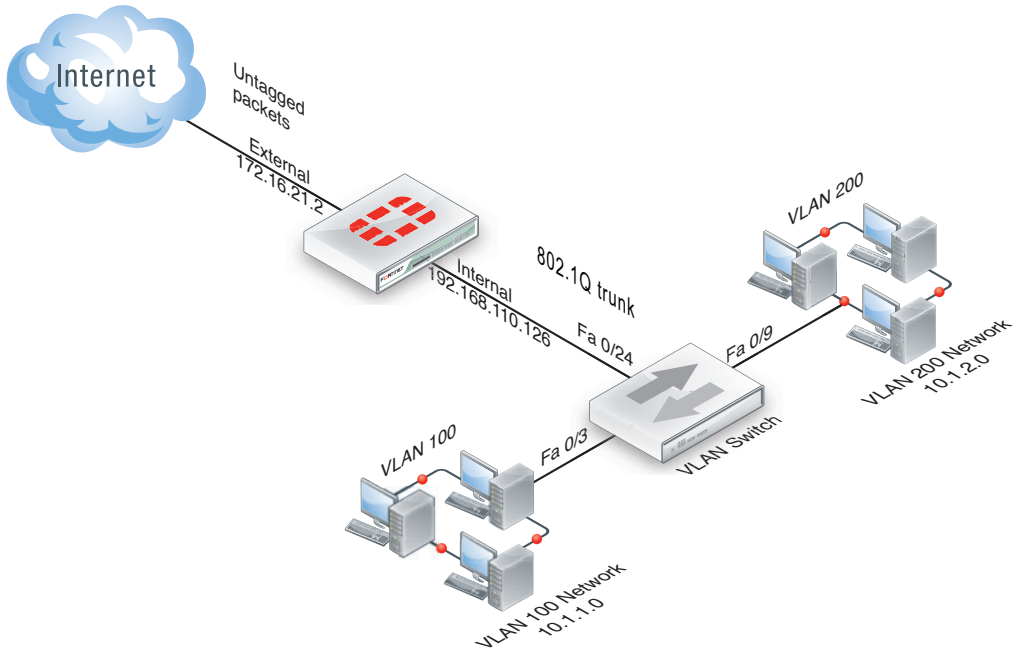
Example VLAN configuration in NAT mode

In this example two different internal VLAN networks share one interface on the FortiGate unit, and share the connection to the Internet. This example shows that two networks can have separate traffic streams while sharing a single interface. This configuration could apply to two departments in a single company, or to different companies.

There are two different internal network VLANs in this example. VLAN_100 is on the 10.1.1.0/255.255.255.0 subnet, and VLAN_200 is on the 10.1.2.0/255.255.255.0 subnet. These VLANs are connected to the VLAN switch, such as a Cisco 2950 Catalyst switch.

The FortiGate internal interface connects to the VLAN switch through an 802.1Q trunk. The internal interface has an IP address of 192.168.110.126 and is configured with two VLAN subinterfaces (VLAN_100 and VLAN_200). The external interface has an IP address of 172.16.21.2 and connects to the Internet. The external interface has no VLAN subinterfaces.

Figure 17: FortiGate unit with VLANs in NAT mode



When the VLAN switch receives packets from VLAN_100 and VLAN_200, it applies VLAN ID tags and forwards the packets of each VLAN both to local ports and to the FortiGate unit across the trunk link. The FortiGate unit has policies that allow traffic to flow between the VLANs, and from the VLANs to the external network.

This section describes how to configure a FortiGate unit and a Cisco Catalyst 2950 switch for this example network topology. The Cisco configuration commands used in this section are IOS commands.

It is assumed that both the FortiGate unit and the Cisco 2950 switch are installed and connected and that basic configuration has been completed. On the switch, you will need to be able to access the CLI to enter commands. Refer to the manual for your FortiGate model as well as the manual for the switch you select for more information.

It is also assumed that no VDOMs are enabled.

General configuration steps

The following steps provide an overview of configuring and testing the hardware used in this example. For best results in this configuration, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Configure the FortiGate unit
   - Configure the external interface
   - Add two VLAN subinterfaces to the internal network interface
   - Add firewall addresses and address ranges for the internal and external networks
   - Add security policies to allow:
     - the VLAN networks to access each other
     - the VLAN networks to access the external network.
2. Configure the VLAN switch

Configure the FortiGate unit

Configuring the FortiGate unit includes:

- Configure the external interface
- Add VLAN subinterfaces
- Add the firewall addresses
- Add the security policies

Configure the external interface

The FortiGate unit's external interface will provide access to the Internet for all internal networks, including the two VLANs.

To configure the external interface - web-based manager

1. Go to *System* > *Network* > *Interface*.
2. Select *Edit* for the external interface.
3. Enter the following information and select *OK*:

Addressing mode	Manual
IP/Network Mask	172.16.21.2/255.255.255.0

To configure the external interface - CLI

```
config system interface
  edit external
    set mode static
    set ip 172.16.21.2 255.255.255.0
end
```

Add VLAN subinterfaces

This step creates the VLANs on the FortiGate unit internal physical interface. The IP address of the internal interface does not matter to us, as long as it does not overlap with the subnets of the VLAN subinterfaces we are configuring on it.

The rest of this example shows how to configure the VLAN behavior on the FortiGate unit, configure the switches to direct VLAN traffic the same as the FortiGate unit, and test that the configuration is correct.

Adding VLAN subinterfaces can be completed through the web-based manager, or the CLI.

To add VLAN subinterfaces - web-based manager

1. Go to *System* > *Network* > *Interface*.
2. Select *Create New*.
3. Enter the following information and select *OK*:

Name	VLAN_100
Interface	internal
VLAN ID	100
Addressing mode	Manual

IP/Network Mask	10.1.1.1/255.255.255.0
Administrative Access	HTTPS, PING, TELNET

4. Select *Create New*.
5. Enter the following information and select *OK*:

Name	VLAN_200
Interface	internal
VLAN ID	200
Addressing mode	Manual
IP/Network Mask	10.1.2.1/255.255.255.0
Administrative Access	HTTPS, PING, TELNET

To add VLAN subinterfaces - CLI

```
config system interface
  edit VLAN_100
    set vdom root
    set interface internal
    set type vlan
    set vlanid 100
    set mode static
    set ip 10.1.1.1 255.255.255.0
    set allowaccess https ping telnet
  next
  edit VLAN_200
    set vdom root
    set interface internal
    set type vlan
    set vlanid 200
    set mode static
    set ip 10.1.2.1 255.255.255.0
    set allowaccess https ping telnet
end
```

Add the firewall addresses

You need to define the addresses of the VLAN subnets for use in security policies. The FortiGate unit provides one default address, “all”, that you can use when a security policy applies to all addresses as a source or destination of a packet. However, using “all” is less secure and should be avoided when possible.

In this example, the “_Net” part of the address name indicates a range of addresses instead of a unique address. When choosing firewall address names, use informative and unique names.

To add the firewall addresses - web-based manager

1. Go to *Firewall Objects* > *Address* > *Addresses*.
2. Select *Create New*.

3. Enter the following information and select *OK*:

Name	VLAN_100_Net
Type	Subnet
Subnet / IP Range	10.1.1.0/255.255.255.0

4. Select *Create New*.
5. Enter the following information and select *OK*:

Name	VLAN_200_Net
Type	Subnet
Subnet / IP Range	10.1.2.0/255.255.255.0

To add the firewall addresses - CLI

```
config firewall address
  edit VLAN_100_Net
    set type ipmask
    set subnet 10.1.1.0 255.255.255.0
  next
  edit VLAN_200_Net
    set type ipmask
    set subnet 10.1.2.0 255.255.255.0
end
```

Add the security policies

Once you have assigned addresses to the VLANs, you need to configure security policies for them to allow valid packets to pass from one VLAN to another and to the Internet.

You can customize the Security Policy display by including some or all columns, and customize the column order onscreen. Due to this feature, security policy screenshots may not appear the same as on your screen.

If you do not want to allow all services on a VLAN, you can create a security policy for each service you want to allow. This example allows all services.

To add the security policies - web-based manager

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Leave the *Policy Type* as *Firewall* and the *Policy Subtype* as *Address*.
3. Enter the following information and select *OK*:

Incoming Interface	VLAN_100
Source Address	VLAN_100_Net
Outgoing Interface	VLAN_200
Destination Address	VLAN_200_Net

Schedule	Always
Service	ALL
Action	ACCEPT
Enable NAT	Enable

4. Select *Create New*.
5. Leave the *Policy Type* as *Firewall* and the *Policy Subtype* as *Address*.
6. Enter the following information and select *OK*:

Incoming Interface	VLAN_200
Source Address	VLAN_200_Net
Outgoing Interface	VLAN_100
Destination Address	VLAN_100_Net
Schedule	Always
Service	ALL
Action	ACCEPT
Enable NAT	Enable

7. Select *Create New*.
8. Leave the *Policy Type* as *Firewall* and the *Policy Subtype* as *Address*.
9. Enter the following information and select *OK*:

Incoming Interface	VLAN_100
Source Address	VLAN_100_Net
Outgoing Interface	external
Destination Address	all
Schedule	Always
Service	ALL
Action	ACCEPT
Enable NAT	Enable

10. Select *Create New*.
11. Leave the *Policy Type* as *Firewall* and the *Policy Subtype* as *Address*.
12. Enter the following information and select *OK*:

Incoming Interface	VLAN_200
Source Address	VLAN_200_Net

Outgoing Interface	external
Destination Address	all
Schedule	Always
Service	ALL
Action	ACCEPT
Enable NAT	Enable

To add the security policies - CLI

```
config firewall policy
  edit 1
    set srcintf VLAN_100
    set srcaddr VLAN_100_Net
    set dstintf VLAN_200
    set dstaddr VLAN_200_Net
    set schedule always
    set service ALL
    set action accept
    set nat enable
    set status enable
  next
  edit 2
    set srcintf VLAN_200
    set srcaddr VLAN_200_Net
    set dstintf VLAN_100
    set dstaddr VLAN_100_Net
    set schedule always
    set service ALL
    set action accept
    set nat enable
    set status enable
  next
  edit 3
    set srcintf VLAN_100
    set srcaddr VLAN_100_Net
    set dstintf external
    set dstaddr all
    set schedule always
    set service ALL
    set action accept
    set nat enable
    set status enable
  next
  edit 4
    set srcintf VLAN_200
    set srcaddr VLAN_200_Net
```

```
        set dstintf external
        set dstaddr all
        set schedule always
        set service ALL
        set action accept
        set nat enable
        set status enable
    end
```

Configure the VLAN switch

On the Cisco Catalyst 2950 Catalyst VLAN switch, you need to define VLANs 100 and 200 in the VLAN database, and then add a configuration file to define the VLAN subinterfaces and the 802.1Q trunk interface.

One method to configure a Cisco switch is to connect over a serial connection to the console port on the switch, and enter the commands at the CLI. Another method is to designate one interface on the switch as the management interface and use a web browser to connect to the switch's graphical interface. For details on connecting and configuring your Cisco switch, refer to the installation and configuration manuals for the switch.

The switch used in this example is a Cisco Catalyst 2950 switch. The commands used are IOS commands. Refer to the switch manual for help with these commands.

To configure the VLAN subinterfaces and the trunk interfaces

Add this file to the Cisco switch:

```
!
interface FastEthernet0/3
switchport access vlan 100
!
interface FastEthernet0/9
switchport access vlan 200
!
interface FastEthernet0/24
switchport trunk encapsulation dot1q
switchport mode trunk
!
```

The switch has the configuration:

Port 0/3	VLAN ID 100
Port 0/9	VLAN ID 200
Port 0/24	802.1Q trunk

To complete the setup, configure devices on VLAN_100 and VLAN_200 with default gateways. The default gateway for VLAN_100 is the FortiGate VLAN_100 subinterface. The default gateway for VLAN_200 is the FortiGate VLAN_200 subinterface.

Test the configuration

Use diagnostic commands, such as `tracert`, to test traffic routed through the FortiGate unit and the Cisco switch.

Testing traffic from VLAN_100 to VLAN_200

In this example, a route is traced between the two internal networks. The route target is a host on VLAN_200.

Access a command prompt on a Windows computer on the VLAN_100 network, and enter the following command:

```
C:\>tracert 10.1.2.2
Tracing route to 10.1.2.2 over a maximum of 30 hops:
  1   <10 ms   <10 ms   <10 ms  10.1.1.1
  2   <10 ms   <10 ms   <10 ms  10.1.2.2
Trace complete.
```

Testing traffic from VLAN_200 to the external network

In this example, a route is traced from an internal network to the external network. The route target is the external network interface of the FortiGate-800 unit.

From VLAN_200, access a command prompt and enter this command:

```
C:\>tracert 172.16.21.2
Tracing route to 172.16.21.2 over a maximum of 30 hops:
  1   <10 ms   <10 ms   <10 ms  10.1.2.1
  2   <10 ms   <10 ms   <10 ms  172.16.21.2
Trace complete.
```

VLANs in transparent mode

In transparent mode, the FortiGate unit behaves like a layer-2 bridge but can still provide services such as antivirus scanning, web filtering, spam filtering and intrusion protection to traffic. There are some limitations in transparent mode in that you cannot use SSL VPN, PPTP/L2TP VPN, DHCP server, or easily perform NAT on traffic. The limits in transparent mode apply to IEEE 802.1Q VLAN trunks passing through the unit.

VLANs and transparent mode

You can insert the FortiGate unit operating in transparent mode into the VLAN trunk without making changes to your network. In a typical configuration, the FortiGate unit internal interface accepts VLAN packets on a VLAN trunk from a VLAN switch or router connected to internal network VLANs. The FortiGate external interface forwards VLAN-tagged packets through another VLAN trunk to an external VLAN switch or router and on to external networks such as the Internet. You can configure the unit to apply different policies for traffic on each VLAN in the trunk.

To pass VLAN traffic through the FortiGate unit, you add two VLAN subinterfaces with the same VLAN ID, one to the internal interface and the other to the external interface. You then create a security policy to permit packets to flow from the internal VLAN interface to the external VLAN interface. If required, you create another security policy to permit packets to flow from the external VLAN interface to the internal VLAN interface. Typically in transparent mode, you do not permit packets to move between different VLANs. Network protection features, such as

spam filtering, web filtering and anti-virus scanning, are applied through the UTM profiles specified in each security policy, enabling very detailed control over traffic.

When the FortiGate unit receives a VLAN-tagged packet at a physical interface, it directs the packet to the VLAN subinterface with the matching VLAN ID. The VLAN tag is removed from the packet, and the FortiGate unit then applies security policies using the same method it uses for non-VLAN packets. If the packet exits the FortiGate unit through a VLAN subinterface, the VLAN ID for that subinterface is added to the packet and the packet is sent to the corresponding physical interface. For a configuration example, see "Example of VLANs in transparent mode" on page 172.

There are two essential steps to configure your FortiGate unit to work with VLANs in transparent mode:

- Add VLAN subinterfaces
- Create security policies

You can also configure the protection profiles that manage antivirus scanning, web filtering and spam filtering. For more information on UTM profiles, see "Unified Threat Management for FortiOS 5.0" on page 2020.

Add VLAN subinterfaces

The VLAN ID of each VLAN subinterface must match the VLAN ID added by the IEEE 802.1Q-compliant router or switch. The VLAN ID can be any number between 1 and 4094, with 0 being used only for high priority frames and 4095 being reserved. You add VLAN subinterfaces to the physical interface that receives VLAN-tagged packets.

For this example, we are creating a VLAN called internal_v225 on the internal interface, with a VLAN ID of 225. Administrative access is enabled for HTTPS and SSH. VDOMs are not enabled.

To add VLAN subinterfaces in transparent mode - web-based manager

1. Go to *System* > *Network* > *Interface*.
2. Select *Create New*.
3. Enter the following information and select *OK*.

Name	internal_v225
Type	VLAN
Interface	internal
VLAN ID	225
Administrative Access	Enable HTTPS, and SSH. These are very secure access methods.
Comments	VLAN 225 on internal interface

The FortiGate unit adds the new subinterface to the interface that you selected.

Repeat steps 2 and 3 to add additional VLANs. You will need to change the *VLAN ID*, *Name*, and possibly *Interface* when adding additional VLANs.

To add VLAN subinterfaces in transparent mode - CLI

```
config system interface
  edit internal_v225
    set interface internal
    set vlanid 225
    set allowaccess HTTPS SSH
    set description "VLAN 225 on internal interface"
    set vdom root
end
```

Create security policies

In transparent mode, the FortiGate unit performs antivirus and antispam scanning on each VLAN's packets as they pass through the unit. You need security policies to permit packets to pass from the VLAN interface where they enter the unit to the VLAN interface where they exit the unit. If there are no security policies configured, no packets will be allowed to pass from one interface to another.

To add security policies for VLAN subinterfaces - web based manager

1. Go to *Firewall Objects* > *Address* > *Addresses*.
2. Select *Create New* to add firewall addresses that match the source and destination IP addresses of VLAN packets.
3. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
4. Leave the *Policy Type* as *Firewall* and the *Policy Subtype* as *Address*.
5. From the *Incoming Interface/Zone* list, select the VLAN interface where packets enter the unit.
6. From the *Outgoing Interface/Zone* list, select the VLAN interface where packets exit the unit.
7. Select the *Source* and *Destination Address* names that you added in step 2.
8. Select *OK*.

To add security policies for VLAN subinterfaces - CLI

```
config firewall address
  edit incoming_VLAN_address
    set associated-interface <incoming_VLAN_interface>
    set type ipmask
    set subnet <IPv4_address_mask)
  next
  edit outgoing_VLAN_address
    set associated-interface <outgoing_VLAN_interface>
    set type ipmask
    set subnet <IPv4_address_mask>
  next
end
config firewall policy
  edit <unused_policy_number>
    set srcintf <incoming_VLAN_interface>
    set srcaddr incoming_VLAN_address
    set destintf <outgoing_VLAN_interface>
```

```
        set destaddr outgoing_VLAN_address
        set service <protocol_to_allow_on VLAN>
        set action ACCEPT
    next
end
```

Example of VLANs in transparent mode

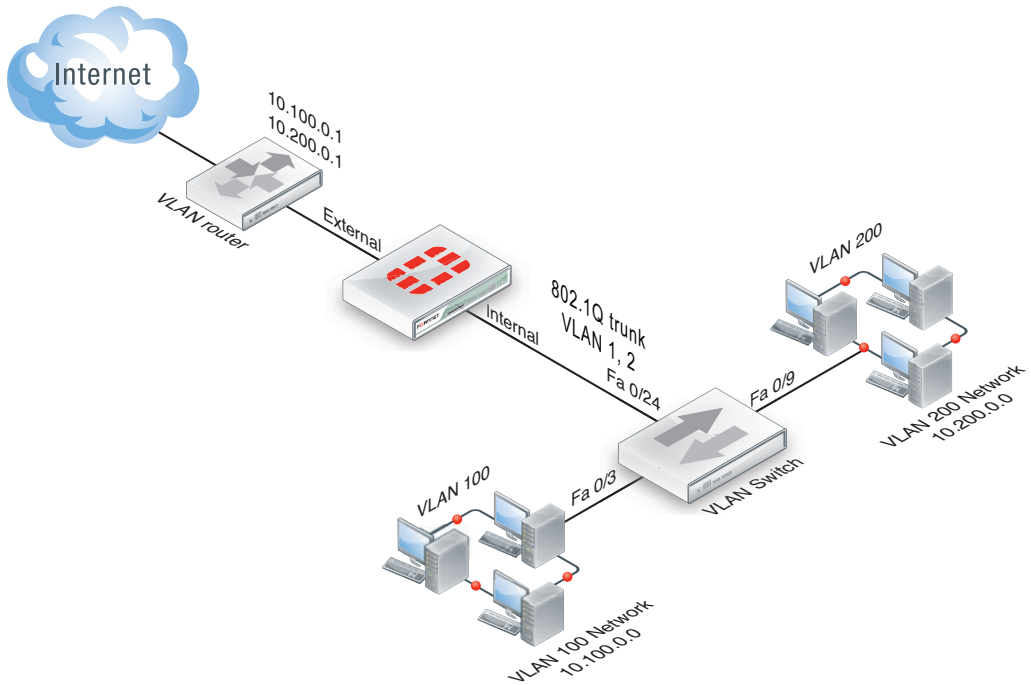
In this example, the FortiGate unit is operating in transparent mode and is configured with two VLANs: one with an ID of 100 and the other with ID 200. The internal and external physical interfaces each have two VLAN subinterfaces, one for VLAN_100 and one for VLAN_200.

The IP range for the internal VLAN_100 network is 10.100.0.0/255.255.0.0, and for the internal VLAN_200 network is 10.200.0.0/255.255.0.0.

The internal networks are connected to a Cisco 2950 VLAN switch, which combines traffic from the two VLANs onto one the FortiGate unit internal interface. The VLAN traffic leaves the FortiGate unit on the external network interface, goes on to the VLAN switch, and on to the Internet. When the FortiGate units receives a tagged packet, it directs it from the incoming VLAN subinterface to the outgoing VLAN subinterface for that VLAN.

This section describes how to configure a FortiGate-800 unit, Cisco switch, and Cisco router in the network topology shown in Figure 180.

Figure 18:VLAN transparent network topology



General configuration steps

The following steps summarize the configuration for this example. For best results, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Configure the FortiGate unit which includes
   - Adding VLAN subinterfaces
   - Adding the security policies
2. Configure the Cisco switch and router

Configure the FortiGate unit

The FortiGate unit must be configured with the VLAN subinterfaces and the proper security policies to enable traffic to flow through the FortiGate unit.

Add VLAN subinterfaces

For each VLAN, you need to create a VLAN subinterface on the internal interface and another one on the external interface, both with the same VLAN ID.

To add VLAN subinterfaces - web-based manager

1. Go to *System* > *Network* > *Interface*.
2. Select *Create New*.
3. Enter the following information and select *OK*:

Name	VLAN_100_int
Interface	internal
VLAN ID	100

4. Select *Create New*.
5. Enter the following information and select *OK*:

Name	VLAN_100_ext
Interface	external
VLAN ID	100

6. Select *Create New*.
7. Enter the following information and select *OK*:

Name	VLAN_200_int
Interface	internal
VLAN ID	200

8. Select *Create New*.
9. Enter the following information and select *OK*:

Name	VLAN_200_ext
Interface	external
VLAN ID	200

To add VLAN subinterfaces - CLI

```
config system interface
  edit VLAN_100_int
    set status down
    set type vlan
    set interface internal
    set vlanid 100
  next
  edit VLAN_100_ext
    set status down
    set type vlan
    set interface external
    set vlanid 100
  next
  edit VLAN_200_int
    set status down
    set type vlan
    set interface internal
    set vlanid 200
  next
  edit VLAN_200_ext
    set status down
    set type vlan
    set interface external
    set vlanid 200
  end
```

Add the security policies

Security policies allow packets to travel between the VLAN_100_int interface and the VLAN_100_ext interface. Two policies are required; one for each direction of traffic. The same is required between the VLAN_200_int interface and the VLAN_200_ext interface, for a total of four required security policies.

To add the security policies - web-based manager

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Leave the *Policy Type* as *Firewall* and the *Policy Subtype* as *Address*.
3. Enter the following information and select *OK*:

Incoming Interface	VLAN_100_int
Source Address	all
Outgoing Interface	VLAN_100_ext
Destination Address	all
Schedule	Always
Service	ALL
Action	ACCEPT

4. Select *Create New*.
5. Leave the *Policy Type* as *Firewall* and the *Policy Subtype* as *Address*.
6. Enter the following information and select *OK*:

Incoming Interface	VLAN_100_ext
Source Address	all
Outgoing Interface	VLAN_100_int
Destination Address	all
Schedule	Always
Service	ALL
Action	ACCEPT

7. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
8. Leave the *Policy Type* as *Firewall* and the *Policy Subtype* as *Address*.
9. Enter the following information and select *OK*:

Incoming Interface	VLAN_200_int
Source Address	all
Outgoing Interface	VLAN_200_ext
Destination Address	all
Schedule	Always
Service	ALL
Action	ACCEPT
Enable NAT	Enable

10. Select *Create New*.
11. Leave the *Policy Type* as *Firewall* and the *Policy Subtype* as *Address*.
12. Enter the following information and select *OK*:

Incoming Interface	VLAN_200_ext
Source Address	all
Outgoing Interface	VLAN_200_int
Destination Address	all
Schedule	Always
Service	ALL
Action	ACCEPT

To add the security policies - CLI

```
config firewall policy
  edit 1
    set srcintf VLAN_100_int
    set srcaddr all
    set dstintf VLAN_100_ext
    set dstaddr all
    set action accept
    set schedule always
    set service ALL
  next
  edit 2
    set srcintf VLAN_100_ext
    set srcaddr all
    set dstintf VLAN_100_int
    set dstaddr all
    set action accept
    set schedule always
    set service ALL
  next
  edit 3
    set srcintf VLAN_200_int
    set srcaddr all
    set dstintf VLAN_200_ext
    set dstaddr all
    set action accept
    set schedule always
    set service ALL
  next
  edit 4
    set srcintf VLAN_200_ext
    set srcaddr all
    set dstintf VLAN_200_int
    set dstaddr all
    set action accept
    set schedule always
    set service ALL
  end
```

Configure the Cisco switch and router

This example includes configuration for the Cisco Catalyst 2900 ethernet switch, and for the Cisco Multiservice 2620 ethernet router. If you have access to a different VLAN enabled switch or VLAN router you can use them instead, however their configuration is not included in this document.

Configure the Cisco switch

On the VLAN switch, you need to define VLAN_100 and VLAN_200 in the VLAN database and then add a configuration file to define the VLAN subinterfaces and the 802.1Q trunk interface.

Add this file to the Cisco switch:

```
interface FastEthernet0/3
 switchport access vlan 100
!
interface FastEthernet0/9
 switchport access vlan 200
!
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
```

The switch has the following configuration:

Port 0/3	VLAN ID 100
Port 0/9	VLAN ID 200
Port 0/24	802.1Q trunk

Configure the Cisco router

You need to add a configuration file to the Cisco Multiservice 2620 ethernet router. The file defines the VLAN subinterfaces and the 802.1Q trunk interface on the router. The 802.1Q trunk is the physical interface on the router.

The IP address for each VLAN on the router is the gateway for that VLAN. For example, all devices on the internal VLAN_100 network will have 10.100.0.1 as their gateway.

Add this file to the Cisco router:

```
!
interface FastEthernet0/0
!
interface FastEthernet0/0.1
 encapsulation dot1Q 100
 ip address 10.100.0.1 255.255.255.0
!
interface FastEthernet0/0.2
 encapsulation dot1Q 200
 ip address 10.200.0.1 255.255.255.0
!
```

The router has the following configuration:

Port 0/0.1	VLAN ID 100
Port 0/0.2	VLAN ID 200
Port 0/0	802.1Q trunk

Test the configuration

Use diagnostic network commands such as traceroute (`tracert`) and ping to test traffic routed through the network.

Testing traffic from VLAN_100 to VLAN_200

In this example, a route is traced between the two internal networks. The route target is a host on VLAN_200. The Windows traceroute command `tracert` is used.

From VLAN_100, access a Windows command prompt and enter this command:

```
C:\>tracert 10.1.2.2
Tracing route to 10.1.2.2 over a maximum of 30 hops:
  1    <10 ms    <10 ms    <10 ms  10.1.1.1
  2    <10 ms    <10 ms    <10 ms  10.1.2.2
Trace complete.
```

Troubleshooting VLAN issues

Several problems can occur with your VLANs. Since VLANs are interfaces with IP addresses, they behave as interfaces and can have similar problems that you can diagnose with tools such as ping, traceroute, packet sniffing, and diag debug.

Asymmetric routing

You might discover unexpectedly that hosts on some networks are unable to reach certain other networks. This occurs when request and response packets follow different paths. If the FortiGate unit recognizes the response packets, but not the requests, it blocks the packets as invalid. Also, if the FortiGate unit recognizes the same packets repeated on multiple interfaces, it blocks the session as a potential attack.

This is asymmetric routing. By default, the FortiGate unit blocks packets or drops the session when this happens. You can configure the FortiGate unit to permit asymmetric routing by using the following CLI commands:

```
config vdom
  edit <vdom_name>
    config system settings
    set asymroute enable
  end
end
```

If VDOMs are enabled, this command is per VDOM. You must set it for each VDOM that has the problem. If this solves your blocked traffic issue, you know that asymmetric routing is the cause. But allowing asymmetric routing is not the best solution, because it reduces the security of your network.

For a long-term solution, it is better to change your routing configuration or change how your FortiGate unit connects to your network. The Asymmetric Routing and Other FortiGate Layer-2

Installation Issues technical note provides detailed examples of asymmetric routing situations and possible solutions.

If you enable asymmetric routing, antivirus and intrusion prevention systems will not be effective. Your FortiGate unit will be unaware of connections and treat each packet individually. It will become a stateless firewall.

Layer-2 and Arp traffic

By default, FortiGate units do not pass layer-2 traffic. If there are layer-2 protocols such as IPX, PPTP or L2TP in use on your network, you need to configure your FortiGate unit interfaces to pass these protocols without blocking. Another type of layer-2 traffic is ARP traffic. For more information on ARP traffic, see "ARP traffic" on page 179.

You can allow these layer-2 protocols using the CLI command:

```
config vdom
  edit <vdom_name>
    config system interface
    edit <name_str>
    set l2forward enable
  end
end
```

where `<name_str>` is the name of an interface.

If VDOMs are enabled, this command is per VDOM. You must set it for each VDOM that has the problem. If you enable layer-2 traffic, you may experience a problem if packets are allowed to repeatedly loop through the network. This repeated looping, very similar to a broadcast storm, occurs when you have more than one layer-2 path to a destination. Traffic may overflow and bring your network to a halt. You can break the loop by enabling Spanning Tree Protocol (STP) on your network's switches and routers. For more information, see "STP forwarding" on page 1262.

ARP traffic

Address Resolution Protocol (ARP) packets are vital to communication on a network, and ARP support is enabled on FortiGate unit interfaces by default. Normally you want ARP packets to pass through the FortiGate unit, especially if it is sitting between a client and a server or between a client and a router.

ARP traffic can cause problems, especially in transparent mode where ARP packets arriving on one interface are sent to all other interfaces including VLAN subinterfaces. Some layer-2 switches become unstable when they detect the same MAC address originating on more than one switch interface or from more than one VLAN. This instability can occur if the layer-2 switch does not maintain separate MAC address tables for each VLAN. Unstable switches may reset and cause network traffic to slow down considerably.

The default ARP timeout value is 5 minutes (300 seconds). This timeout is not configurable.

Usually ARP entries are removed after 5 minutes. However, some conditions can cause ARP entries to remain for a longer time. Enter the `get system arp` CLI command to view the entries in the ARP list.

Multiple VDOMs solution

By default, physical interfaces are in the root domain. If you do not configure any of your VLANs in the root VDOM, it will not matter how many interfaces are in the root VDOM.

The multiple VDOMs solution is to configure multiple VDOMs on the FortiGate unit, one for each VLAN. In this solution, you configure one inbound and one outbound VLAN interface in each VDOM. ARP packets are not forwarded between VDOMs. This configuration limits the VLANs in a VDOM and correspondingly reduces the administration needed per VDOM.

As a result of this configuration, the switches do not receive multiple ARP packets with duplicate MACs. Instead, the switches receive ARP packets with different VLAN IDs and different MACs. Your switches are stable.

However, you should ***not*** use the multiple VDOMs solution under any of the following conditions:

- you have more VLANs than licensed VDOMs
- you do not have enough physical interfaces

Instead, use one of two possible solutions, depending on which operation mode you are using:

- In NAT mode, you can use the `vlan forward` CLI command.
- In transparent mode, you can use the `forward-domain` CLI command. But you still need to be careful in some rare configurations.

Vlanforward solution

If you are using NAT mode, the solution is to use the `vlanforward` CLI command for the interface in question. By default, this command is enabled and will forward VLAN traffic to all VLANs on this interface. When disabled, each VLAN on this physical interface can send traffic only to the same VLAN. There is no cross-talk between VLANs, and ARP packets are forced to take one path along the network which prevents the multiple paths problem.

In the following example, `vlanforward` is disabled on port1. All VLANs configured on port1 will be separate and will not forward any traffic to each other.

```
config system interface
  edit port1
    set vlanforward disable
end
```

Forward-domain solution

If you are using transparent mode, the solution is to use the `forward-domain` CLI command. This command tags VLAN traffic as belonging to a particular collision group, and only VLANs tagged as part of that collision group receive that traffic. It is like an additional set of VLANs. By default, all interfaces and VLANs are part of forward-domain collision group 0. The many benefits of this solution include reduced administration, the need for fewer physical interfaces, and the availability of more flexible network solutions.

In the following example, forward-domain collision group 340 includes VLAN 340 traffic on port1 and untagged traffic on port 2. Forward-domain collision group 341 includes VLAN 341 traffic on port 1 and untagged traffic on port 3. All other interfaces are part of forward-domain collision group 0 by default. This configuration separates VLANs 340 and 341 from each other on port 1, and prevents the ARP packet problems from before.

Use these CLI commands:

```
config system interface
  edit port1
```

```
    next
    edit port2
      set forward_domain 340
    next
    edit port3
      set forward_domain 341
    next
    edit port1-340
      set forward_domain 340
      set interface port1
      set vlanid 340
    next
    edit port1-341
      set forward_domain 341
      set interface port1
      set vlanid 341
end
```

You may experience connection issues with layer-2 traffic, such as ping, if your network configuration has:

- packets going through the FortiGate unit in transparent mode more than once
- more than one forwarding domain (such as incoming on one forwarding domain and outgoing on another)
- IPS and AV enabled.

Now IPS and AV is applied the first time packets go through the FortiGate unit, but not on subsequent passes. Only applying IPS and AV to this first pass fixes the network layer-2 related connection issues.

NetBIOS

Computers running Microsoft Windows operating systems that are connected through a network rely on a WINS server to resolve host names to IP addresses. The hosts communicate with the WINS server by using the NetBIOS protocol.

To support this type of network, you need to enable the forwarding of NetBIOS requests to a WINS server. The following example will forward NetBIOS requests on the internal interface for the WINS server located at an IP address of 192.168.111.222.

```
config system interface
  edit internal
    set netbios_forward enable
    set wins-ip 192.168.111.222
end
```

These commands apply only in NAT mode. If VDOMs are enabled, these commands are per VDOM. You must set them for each VDOM that has the problem.

STP forwarding

The FortiGate unit does not participate in the Spanning Tree Protocol (STP). STP is an IEEE 802.1 protocol that ensures there are no layer-2 loops on the network. Loops are created when there is more than one route for traffic to take and that traffic is broadcast back to the original switch. This loop floods the network with traffic, reducing available bandwidth to nothing.

If you use your FortiGate unit in a network topology that relies on STP for network loop protection, you need to make changes to your FortiGate configuration. Otherwise, STP recognizes your FortiGate unit as a blocked link and forwards the data to another path. By default, your FortiGate unit blocks STP as well as other non-IP protocol traffic.

Using the CLI, you can enable forwarding of STP and other layer-2 protocols through the interface. In this example, layer-2 forwarding is enabled on the external interface:

```
config system interface
  edit external
    set l2forward enable
    set stpforward enable
end
```

By substituting different commands for `stpforward enable`, you can also allow layer-2 protocols such as IPX, PPTP or L2TP to be used on the network. For more information, see "Layer-2 and Arp traffic" on page 179.

Too many VLAN interfaces

Any virtual domain can have a maximum of 255 interfaces in transparent mode. This includes VLANs, other virtual interfaces, and physical interfaces. NAT mode supports from 255 to 8192 depending on the FortiGate model. This total number of interfaces includes VLANs, other virtual interfaces, and physical interfaces.

Your FortiGate unit may allow you to configure more interfaces than this. However, if you configure more than 255 interfaces, your system will become unstable and, over time, will not work properly. As all interfaces are used, they will overflow the routing table that stores the interface information, and connections will fail. When you try to add more interfaces, an error message will state that the maximum limit has already been reached.

If you see this error message, chances are you already have too many VLANs on your system and your routing has become unstable. To verify, delete a VLAN and try to add it back. If you have too many, you will not be able to add it back on to the system. In this case, you will need to remove enough interfaces (including VLANs) so that the total number of interfaces drops to 255 or less. After doing this, you should also reboot your FortiGate unit to clean up its memory and buffers, or you will continue to experience unstable behavior.

To configure more than 255 interfaces on your FortiGate unit in transparent mode, you have to configure multiple VDOMs, each with many VLANs. However, if you want to create more than the default 10 VDOMs (or a maximum of 2550 interfaces), you must buy a license for additional VDOMs.

With these extra licenses, you can configure up to 500 VDOMs, with each VDOM containing up to 255 VLANs in transparent mode. This is a theoretical maximum of over 127 500 interfaces. However, system resources will quickly get used up before reaching that theoretical maximum. To achieve the maximum number of VDOMs, you need to have top-end hardware with the most resources possible.

In NAT mode, if you have a top-end model, the maximum interfaces per VDOM can be as high as 8192, enough for all the VLANs in your configuration.

Your FortiGate unit has limited resources, such as CPU load and memory, that are divided between all configured VDOMs. When running 250 or more VDOMs, you may need to monitor the system resources to ensure there is enough to support the configured traffic processing.

PPTP and L2TP

A virtual private network (VPN) is a way to use a public network, such as the Internet, as a vehicle to provide remote offices or individual users with secure access to private networks. FortiOS supports the Point-to-Point Tunneling Protocol (PPTP), which enables interoperability between FortiGate units and Windows or Linux PPTP clients. Because FortiGate units support industry standard PPTP VPN technologies, you can configure a PPTP VPN between a FortiGate unit and most third-party PPTP VPN peers.

This section describes how to configure PPTP and L2TP VPNs as well as PPTP passthrough.

This section includes the topics:

How PPTP VPNs work

The Point-to-Point Tunneling Protocol enables you to create a VPN between a remote client and your internal network. Because it is a Microsoft Windows standard, PPTP does not require third-party software on the client computer. As long as the ISP supports PPTP on its servers, you can create a secure connection by making relatively simple configuration changes to the client computer and the FortiGate unit.

PPTP uses Point-to-Point protocol (PPP) authentication protocols so that standard PPP software can operate on tunneled PPP links. PPTP packages data in PPP packets and then encapsulates the PPP packets within IP packets for transmission through a VPN tunnel.

When the FortiGate unit acts as a PPTP server, a PPTP session and tunnel is created as soon as the PPTP client connects to the FortiGate unit. More than one PPTP session can be supported on the same tunnel. FortiGate units support PAP, CHAP, and plain text authentication. PPTP clients are authenticated as members of a user group.

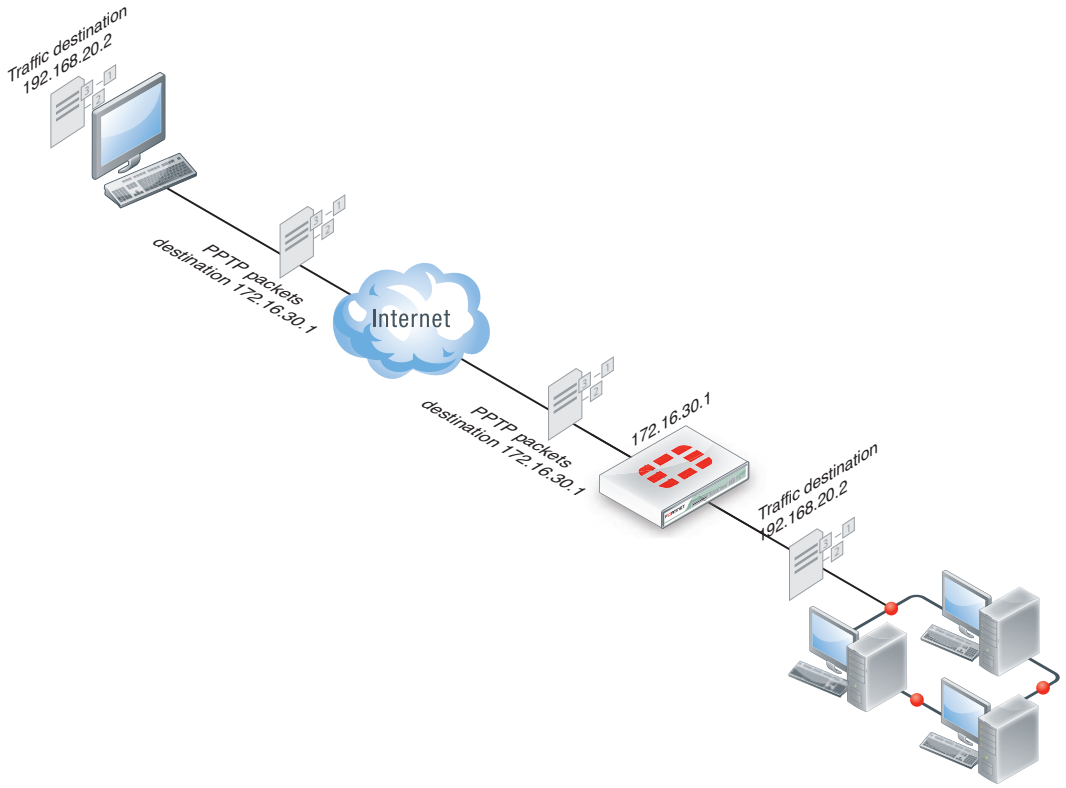
Traffic from one PPTP peer is encrypted using PPP before it is encapsulated using Generic Routing Encapsulation (GRE) and routed to the other PPTP peer through an ISP network. PPP packets from the remote client are addressed to a computer on the private network behind the FortiGate unit. PPTP packets from the remote client are addressed to the public interface of the FortiGate unit. See Figure 19 on page 184

.

PPTP control channel messages are not authenticated, and their integrity is not protected. Furthermore, encapsulated PPP packets are not cryptographically protected and may be read or modified unless appropriate encryption software such as Secure Shell (SSH) or Secure File Transfer Protocol (SFTP) is used to transfer data after the tunnel has been established.

As an alternative, you can use encryption software such as Microsoft Point-to-Point Encryption (MPPE) to secure the channel. MPPE is built into Microsoft Windows clients and can be installed on Linux clients. FortiGate units support MPPE.

Figure 19: Packet encapsulation



In Figure 19, traffic from the remote client is addressed to a computer on the network behind the FortiGate unit. When the PPTP tunnel is established, packets from the remote client are encapsulated and addressed to the FortiGate unit. The FortiGate unit forwards disassembled packets to the computer on the internal network.

When the remote PPTP client connects, the FortiGate unit assigns an IP address from a reserved range of IP addresses to the client PPTP interface. The PPTP client uses the assigned IP address as its source address for the duration of the connection.

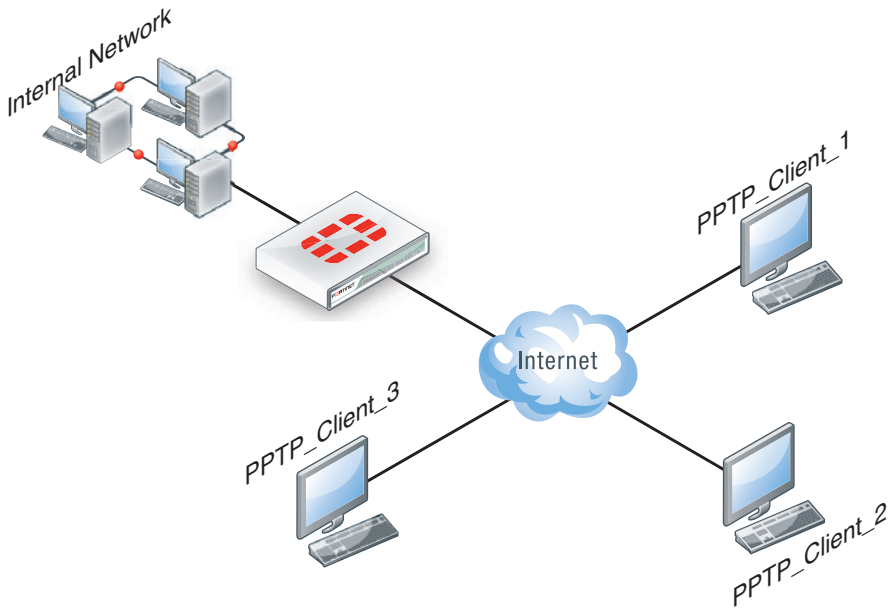
When the FortiGate unit receives a PPTP packet, the unit disassembles the PPTP packet and forwards the packet to the correct computer on the internal network. The security policy and protection profiles on the FortiGate unit ensure that inbound traffic is screened and processed securely.

PPTP clients must be authenticated before a tunnel is established. The authentication process relies on FortiGate user group definitions, which can optionally use established authentication mechanisms such as RADIUS or LDAP to authenticate PPTP clients. All PPTP clients are challenged when a connection attempt is made.

FortiGate unit as a PPTP server

In the most common Internet scenario, the PPTP client connects to an ISP that offers PPP connections with dynamically-assigned IP addresses. The ISP forwards PPTP packets to the Internet, where they are routed to the FortiGate unit.

Figure 20: FortiGate unit as a PPTP server



If the FortiGate unit will act as a PPTP server, there are a number of steps to complete:

- Configure user authentication for PPTP clients.
- Enable PPTP.
- Specify the range of addresses that are assigned to PPTP clients when connecting
- Configure the security policy.

Configuring user authentication for PPTP clients

To enable authentication for PPTP clients, you must create user accounts and a user group to identify the PPTP clients that need access to the network behind the FortiGate unit. Within the user group, you must add a user for each PPTP client.

You can choose to use a plain text password for authentication or forward authentication requests to an external RADIUS, LDAP, or TACACS+ server. If password protection will be provided through a RADIUS, LDAP, or TACACS+ server, you must configure the FortiGate unit to forward authentication requests to the authentication server.

This example creates a basic user/password combination.

Configuring a user account

To add a local user - web-based manager

1. Go to *User & Device* > *User* > *User Definition* and select *Create New.*
2. Enter a *User Name*.
3. Enter a *Password* for the user. The password should be at least six characters.
4. Select *OK*.

To add a local user - CLI

```
config user local
  edit <username>
    set type password
    set passwd <password>
end
```

Configuring a user group

To ease configuration, create user groups that contain users in similar categories or departments.

To create a user group - web-based manager

1. Go to *User & Device* > *User* > *User Group* and select *Create New*.
2. Enter a *Name* for the group.
3. Select the *Type* of *Firewall*.
4. From the *Available Users* list, select the required users and select the right-facing arrow to add them to the *Members* list.
5. Select *OK*.

To create a user group - CLI

```
config user group
  edit <group_name>
    set group-type firewall
    set members <user_names>
end
```

Enabling PPTP and specifying the PPTP IP address range

The PPTP address range specifies the range of addresses reserved for remote PPTP clients. When a PPTP client connects to the FortiGate unit, the client is assigned an IP address from this range. Afterward, the FortiGate unit uses the assigned address to communicate with the PPTP client.

The address range that you reserve can be associated with private or routable IP addresses. If you specify a private address range that matches a network behind the FortiGate unit, the assigned address will make the PPTP client appear to be part of the internal network.

PPTP requires two IP addresses, one for each end of the tunnel. The PPTP address range is the range of addresses reserved for remote PPTP clients. When the remote PPTP client establishes a connection, the FortiGate unit assigns an IP address from the reserved range of IP addresses to the client PPTP interface or retrieves the assigned IP address from the PPTP user group. If you use the PPTP user group, you must also define the FortiGate end of the tunnel by entering the IP address of the unit in *Local IP* (web-based manager) *or* `local-ip` (CLI). The PPTP client uses the assigned IP address as its source address for the duration of the connection.

PPTP configuration is only available through the CLI. In the example below, PPTP is enabled with the use of an IP range of `182.168.1.1` to `192.168.1.10` for addressing.

The start and end IPs in the PPTP address range must be in the same 24-bit subnet, for example, 192.168.1.1 - 192.168.1.254.

```
config vpn pptp
  set status enable
  set ip-mode range
  set eip 192.168.1.10
  set sip 192.168.1.1
end
```

In this example, PPTP is enabled with the use of a user group for addressing, where the IP address of the PPTP server is `192.168.1.2` and the user group is `hr_admin`.

```
config vpn pptp
  set status enable
  set ip-mode range
  set local-ip 192.168.2.1
  set usrgrp hr_admin
end
```

Adding the security policy

The security policy specifies the source and destination addresses that can generate traffic inside the PPTP tunnel and defines the scope of services permitted through the tunnel. If a selection of services are required, define a service group.

To configure the firewall for the PPTP tunnel - web-based manager

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Leave the *Policy Type* as *Firewall* and the *Policy Subtype* as *Address*.
3. Complete the following and select *OK*:

Incoming Interface	The FortiGate interface connected to the Internet.
Source Address	Select the name that corresponds to the range of addresses that you reserved for PPTP clients.
Outgoing Interface	The FortiGate interface connected to the internal network.
Destination Address	Select the name that corresponds to the IP addresses behind the FortiGate unit.
Schedule	always
Service	ALL
Action	ACCEPT

Do not select identity-based policy, as this will cause the PPTP access to fail. Authentication is configured in the PPTP configuration setup

To configure the firewall for the PPTP tunnel - CLI

```
config firewall policy
  edit 1
    set srcintf <interface to internet>
    set dstintf <interface to internal network>
    set srcaddr <reserved_range>
    set dstaddr <internal_addresses>
    set action accept
    set schedule always
    set service ALL
end
```

Configuring the FortiGate unit for PPTP VPN

To arrange for PPTP packets to pass through the FortiGate unit to an external PPTP server, perform the following tasks in the order given:

- Configure user authentication for PPTP clients.
- Enable PPTP on the FortiGate unit and specify the range of addresses that can be assigned to PPTP clients when they connect.
- Configure PPTP pass through on the FortiGate unit.

Configuring the FortiGate unit for PPTP pass through

To forward PPTP packets to a PPTP server on the network behind the FortiGate unit, you need to perform the following configuration tasks on the FortiGate unit:

- Define a virtual IP address that points to the PPTP server.
- Create a security policy that allows incoming PPTP packets to pass through to the PPTP server.

The address range is the external (public) ip address range which requires access to the internal PPTP server through the FortiGate virtual port-forwarding firewall.

IP addresses used in this document are fictional and follow the technical documentation guidelines specific to Fortinet. Real external IP addresses are not used.

Configuring a virtual IP address

The virtual IP address will be the address of the PPTP server host.

To define a virtual IP for PPTP pass through - web-based manager

1. Go to *Firewall Objects* > *Virtual IP* > *Virtual IP*.
2. Select *Create New*.
3. Enter the name of the VIP, for example, `PPTP_Server`.
4. Select the *External Interface* where the packets will be received for the PPTP server.
5. Enter the *External IP Address* for the VIP.
6. Select *Port Forwarding*.
7. Set the *Protocol to TCP*.

8. Enter the *External Service Port* of `1723`, the default for PPTP.
9. Enter the *Map to Port* to `1723`.
10. Select *OK*.

To define a virtual IP for PPTP pass through - web-based manager

```
config firewall vip
  edit PPTP_Server
    set extinf <interface>
    set extip <ip_address>
    set portforward enable
    set protocol tcp
    set extport 1723
    set mappedport 1723
end
```

Configuring a port-forwarding security policy

To create a port-forwarding security policy for PPTP pass through you must first create an address range reserved for the PPTP clients.

To create an address range - web-based manager

1. Go to *Firewall Objects* > *Address* > *Addresses* and select *Create New*.
2. Enter a *Name* for the range, for example, `External_PPTP`.
3. Select a *Type* of *Subnet/IP Range*.
4. Enter the IP address range.
5. Select the *Interface* to the Internet.
6. Select *OK*.

To create an address range - CLI

```
config firewall address
  edit External_PPTP
    set iprange <ip_range>
    set start-ip <ip_address>
    set end-ip <ip_address>
    set associated-interface <internet_interface>
end
```

With the address set, you can add the security policy.

To add the security policy - web-based manager

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Leave the *Policy Type* as *Firewall* and the *Policy Subtype* as *Address*.
3. Complete the following and select *OK*:

Incoming Interface	The FortiGate interface connected to the Internet.
Source Address	Select the address range created in the previous step.
Outgoing Interface	The FortiGate interface connected to the PPTP server.
Destination Address	Select the VIP address created in the previous steps.

Schedule	always
Service	PPTP
Action	ACCEPT

To add the security policy - CLI

```
config firewall policy
  edit <policy_number>
    set srcintf <interface to internet>
    set dstintf <interface to PPTP server>
    set srcaddr <address_range>
    set dstaddr <PPTP_server_address>
    set action accept
    set schedule always
    set service PPTP
end
```

Testing PPTP VPN connections

To confirm that a PPTP VPN between a local network and a dialup client has been configured correctly, at the dialup client, issue a ping command to test the connection to the local network. The PPTP VPN tunnel initializes when the dialup client attempts to connect.

Logging VPN events

PPTP VPN, activity is logged when enabling VPN logging. The FortiGate unit connection events and tunnel status (up/down) are logged.

To log VPN events

1. Go to *Log & Report* > *Log Config* > *Log Settings*.
2. Enable the storage of log messages to one or more locations.
3. Select *VPN activity event*.
4. Select *Apply*.

To view event logs

1. Go to *Log & Report* > *Event Log* > *VPN*.
2. If the option is available from the Log Type list, select the log file from disk or memory.

Configuring L2TP VPNs

This section describes how to configure a FortiGate unit to establish a Layer Two Tunneling Protocol (L2TP) tunnel with a remote dialup client. The FortiGate implementation of L2TP enables a remote dialup client to establish an L2TP tunnel with the FortiGate unit directly.

According to RFC 2661, an Access Concentrator (LAC) can establish an L2TP tunnel with an L2TP Network Server (LNS). In a typical scenario, the LAC is managed by an ISP and located on the ISP premises; the LNS is the gateway to a private network. When a remote dialup client connects to the Internet through the ISP, the ISP uses a local database to establish the identity

of the caller and determine whether the caller needs access to an LNS through an L2TP tunnel. If the services registered to the caller indicate that an L2TP connection to the LNS is required, the ISP LAC attempts to establish an L2TP tunnel with the LNS.

A FortiGate unit can be configured to act as an LNS. The FortiGate implementation of L2TP enables a remote dialup client to establish an L2TP tunnel with the FortiGate unit directly, bypassing any LAC managed by an ISP. The ISP must configure its network access server to forward L2TP traffic from the remote client to the FortiGate unit directly whenever the remote client requires an L2TP connection to the FortiGate unit.

When the FortiGate unit acts as an LNS, an L2TP session and tunnel is created as soon as the remote client connects to the FortiGate unit. The FortiGate unit assigns an IP address to the client from a reserved range of IP addresses. The remote client uses the assigned IP address as its source address for the duration of the connection.

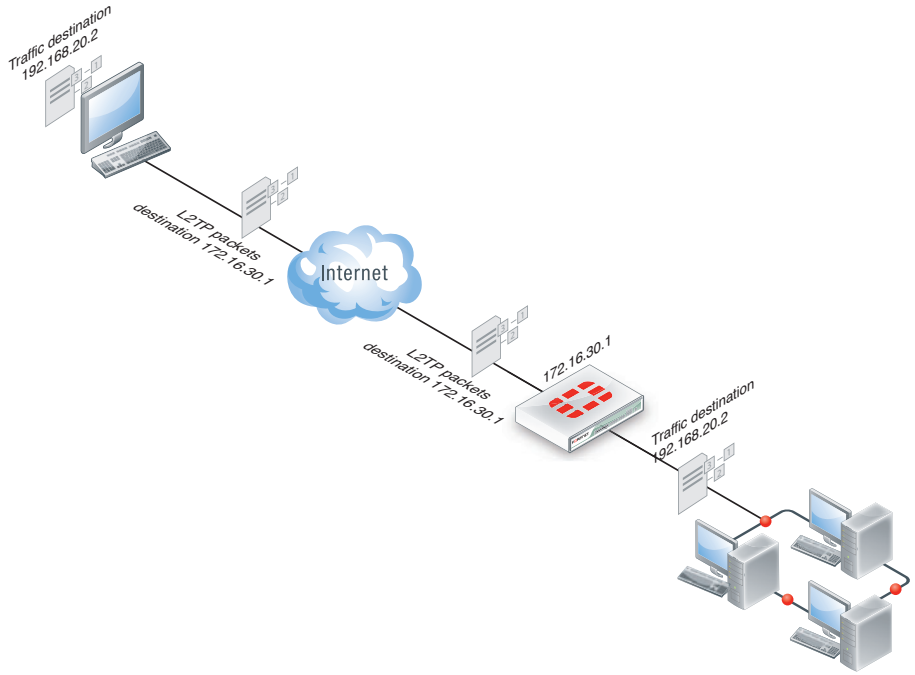
More than one L2TP session can be supported on the same tunnel. FortiGate units can be configured to authenticate remote clients using a plain text user name and password, or authentication can be forwarded to an external RADIUS or LDAP server. L2TP clients are authenticated as members of a user group.

FortiGate units support L2TP with Microsoft Point-to-Point Encryption (MPPE) encryption only. Later implementations of Microsoft L2TP for Windows use IPSec and require certificates for authentication and encryption. If you want to use Microsoft L2TP with IPSec to connect to a FortiGate unit, the IPSec and certificate elements must be disabled on the remote client

Traffic from the remote client must be encrypted using MPPE before it is encapsulated and routed to the FortiGate unit. Packets originating at the remote client are addressed to a computer on the private network behind the FortiGate unit. Encapsulated packets are addressed to the public interface of the FortiGate unit. See Figure 21.

When the FortiGate unit receives an L2TP packet, the unit disassembles the packet and forwards the packet to the correct computer on the internal network. The security policy and protection profiles on the FortiGate unit ensure that inbound traffic is screened and processed securely.

Figure 21:L2TP encapsulation

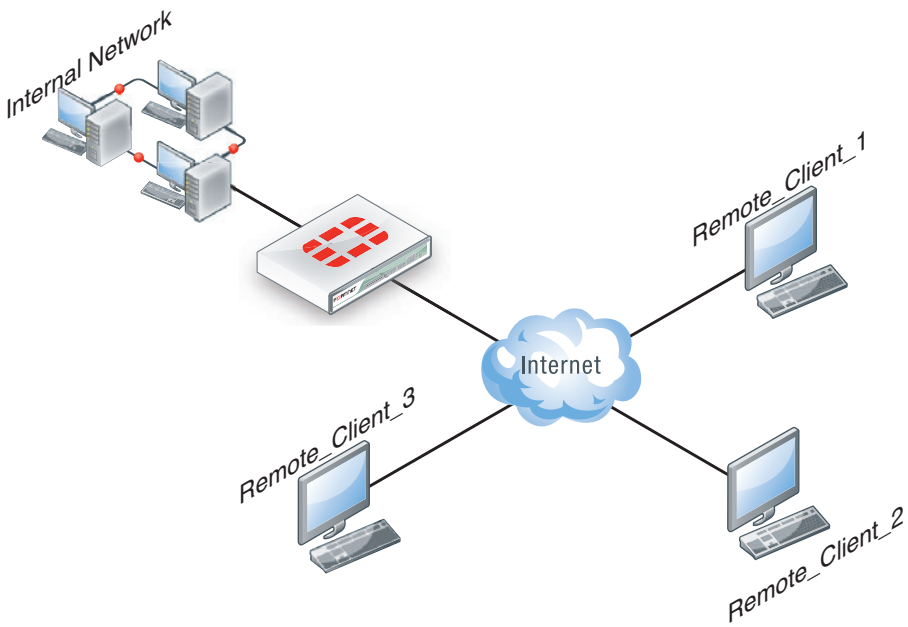


FortiGate units cannot deliver non-IP traffic such as Frame Relay or ATM frames encapsulated in L2TP packets — FortiGate units support the IPv4 and IPv6 addressing schemes only

Network topology

The remote client connects to an ISP that determines whether the client requires an L2TP connection to the FortiGate unit. If an L2TP connection is required, the connection request is forwarded to the FortiGate unit directly.

Figure 22: Example L2TP configuration



L2TP infrastructure requirements

- The FortiGate unit must be operating in NAT mode and have a static public IP address.
- The ISP must configure its network access server to forward L2TP traffic from remote clients to the FortiGate unit directly.
- The remote client must not generate non-IP traffic (Frame Relay or ATM frames).
- The remote client includes L2TP support with MPPE encryption. If the remote client includes Microsoft L2TP with IPSec, the IPSec and certificate components must be disabled.

L2TP configuration overview

To configure a FortiGate unit to act as an LNS, you perform the following tasks:

- Create an L2TP user group containing one user for each remote client.
- Enable L2TP on the FortiGate unit and specify the range of addresses that can be assigned to remote clients when they connect.
- Define firewall source and destination addresses to indicate where packets transported through the L2TP tunnel will originate and be delivered.
- Create the security policy and define the scope of permitted services between the source and destination addresses.
- Configure the remote clients.

Authenticating L2TP clients

L2TP clients must be authenticated before a tunnel is established. The authentication process relies on FortiGate user group definitions, which can optionally use established authentication mechanisms such as RADIUS or LDAP to authenticate L2TP clients. All L2TP clients are challenged when a connection attempt is made.

To enable authentication, you must create user accounts and a user group to identify the L2TP clients that need access to the network behind the FortiGate unit.

You can choose to use a plain text password for authentication or forward authentication requests to an external RADIUS or LDAP server. If password protection will be provided through a RADIUS or LDAP server, you must configure the FortiGate unit to forward authentication requests to the authentication server.

Enabling L2TP and specifying an address range

The L2TP address range specifies the range of addresses reserved for remote clients. When a remote client connects to the FortiGate unit, the client is assigned an IP address from this range. Afterward, the FortiGate unit uses the assigned address to communicate with the remote client.

The address range that you reserve can be associated with private or routable IP addresses. If you specify a private address range that matches a network behind the FortiGate unit, the assigned address will make the remote client appear to be part of the internal network.

To enable L2TP and specify the L2TP address range, use the `config vpn l2tp` CLI command.

The following example shows how to enable L2TP and set the L2TP address range using a starting address of `192.168.10.80` and an ending address of `192.168.10.100` for an existing group of L2TP users named `L2TP_users`:

```
config vpn l2tp
  set sip 192.168.10.80
  set eip 192.168.10.100
  set status enable
  set usrgrp L2TP_users
end
```

Defining firewall source and destination addresses

Before you define the security policy, you must define the source and destination addresses of packets that are to be transported through the L2TP tunnel:

- For the source address, enter the range of addresses that you reserved for remote L2TP clients (for example `192.168.10.[80-100]`).
- For the destination address, enter the IP addresses of the computers that the L2TP clients need to access on the private network behind the FortiGate unit (for example, `172.16.5.0/24` for a subnet, or `172.16.5.1` for a server or host, or `192.168.10.[10-15]` for an IP address range).

To define the firewall source address

1. Go to *Firewall Objects* > *Address* > *Addresses* and select *Create New*.
2. In the *Address Name* field, type a name that represents the range of addresses that you reserved for remote clients (for example, `Ext_L2TPrange`).
3. In *Type*, select *Subnet / IP Range*.

4. In the *Subnet / IP Range* field, type the corresponding IP address range.
5. In *Interface*, select the FortiGate interface that connects to the clients.
6. This is usually the interface that connects to the Internet.
7. Select *OK*.

To define the firewall destination address

1. Go to *Firewall Objects* > *Address* > *Addresses* and select *Create New*.
2. In the *Address Name* field, type a name that represents a range of IP addresses on the network behind the FortiGate unit (for example, `Int_L2TPaccess`).
3. In *Type*, select *Subnet / IP Range*.
4. In the *Subnet / IP Range* field, type the corresponding IP address range.
5. In *Interface*, select the FortiGate interface that connects to the network behind the FortiGate unit.
6. Select *OK*.

Adding the security policy

The security policy specifies the source and destination addresses that can generate traffic inside the L2TP tunnel and defines the scope of services permitted through the tunnel. If a selection of services are required, define a service group.

To define the traffic and services permitted inside the L2TP tunnel

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Leave the *Policy Type* as *Firewall* and the *Policy Subtype* as *Address*.
3. Enter these settings:

Incoming Interface	Select the FortiGate interface to the Internet.
Source Address	Select the name that corresponds to the address range that reserved for L2TP clients (for example, `Ext_L2TPrange`).
Outgoing Interface	Select the FortiGate interface to the internal (private) network.
Destination Address	Select the name that corresponds to the IP addresses behind the FortiGate unit (for example, `Int_L2TPaccess`).
Service	Select ALL, or if selected services are required instead, select the service group that you defined previously.
Action	ACCEPT

4. Select *OK*.

Configuring a Linux client

This procedure outlines how to install L2TP client software and run an L2TP tunnel on a Linux computer. Obtain an L2TP client package that meets your requirements (for example, `rp-l2tp`). If needed to encrypt traffic, obtain L2TP client software that supports encryption using MPPE.

To establish an L2TP tunnel with a FortiGate unit that has been set up to accept L2TP connections, you can obtain and install the client software following these guidelines:

1. If encryption is required but MPPE support is not already present in the kernel, download and install an MPPE kernel module and reboot your computer.
2. Download and install the L2TP client package.
3. Configure an L2TP connection to run the L2TP program.
4. Configure routes to determine whether all or some of your network traffic will be sent through the tunnel. You must define a route to the remote network over the L2TP link and a host route to the FortiGate unit.
5. Run `l2tpd` to start the tunnel.

Follow the software supplier's documentation to complete the steps.

To configure the system, you need to know the public IP address of the FortiGate unit, and the user name and password that has been set up on the FortiGate unit to authenticate L2TP clients. Contact the FortiGate administrator if required to obtain this information.

Monitoring L2TP sessions

You can display a list of all active sessions and view activity by port number. By default, port 1701 is used for L2TP VPN-related communications. If required, active sessions can be stopped from this view. Use the Top Sessions Dashboard Widget.

Testing L2TP VPN connections

To confirm that a VPN between a local network and a dialup client has been configured correctly, at the dialup client, issue a ping command to test the connection to the local network. The VPN tunnel initializes when the dialup client attempts to connect.

Logging L2TP VPN events

You can configure the FortiGate unit to log VPN events. For L2TP VPNs, connection events and tunnel status (up/down) are logged.

To log VPN events - web-based manager

1. Go to *Log & Report* > *Log Config* > *Log Settings*.
2. Enable the storage of log messages to one or more locations.
3. Select *Enable*, and then select *VPN activity event*.
4. Select *Apply*.

To log VPN events - CLI

```
config log memory setting
  set diskfull overright
  set status enable
end
config log eventfilter
  set ppp
end
```

Advanced concepts

This chapter provides configuration concepts and techniques to enhance your network security.

This section includes the topics:

Dual internet connections (redundant Internet connections)

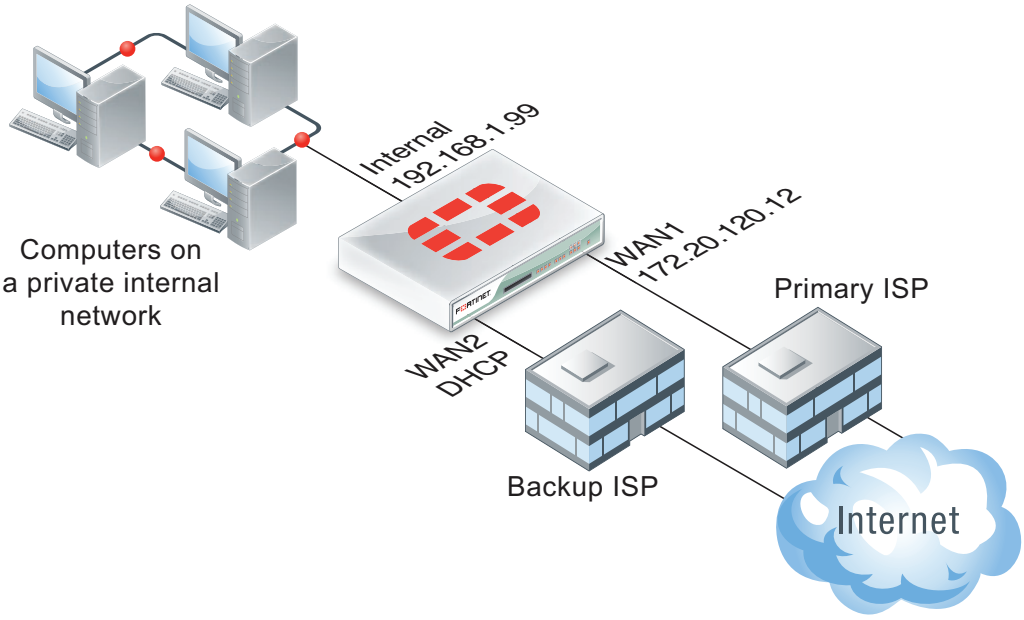
Dual internet connection, dual WAN, or redundant internet connection refers to using two FortiGate interfaces to connect to the Internet. Dual internet connections can be used in three ways:

- redundant interfaces, should one interface go down, the second automatically becomes the main internet connection
- for load sharing to ensure better throughput.
- a combination of redundancy and load sharing.

Redundant interfaces

Redundant interfaces, ensures that should your internet access be no longer available through a certain port, the FortiGate unit will use an alternate port to connect to the Internet.

Figure 23: Configuring redundant interfaces



In this scenario, two interfaces, WAN1 and WAN2 are connected to the Internet using two different ISPs. WAN1 is the primary connection. In an event of a failure of WAN1, WAN2 automatically becomes the connection to the Internet. For this configuration to function correctly, you need to configure three specific settings:

- configure a ping server to determine when the primary interface (WAN1) is down and when the connection returns
- configure a default route for each interface.
- configure security policies to allow traffic through each interface to the internal network.

Ping server

Adding a ping server is required for routing fail over traffic. A ping server will confirm the connectivity of the device's interface

To add a ping server - web-based manager

1. Go to *Router* > *Static* > *Settings* and select *Create New*.

   For low-end FortiGate units, go to *System* > *Network* > *Routing* and select *Create New*.
2. Select the *Interface* that will send ping requests.
3. For the *Ping Server* field, enter the IP address of a server that the FortiGate unit will send ping requests to. This is typically a next hop router or gateway device.
4. Select the *Detect Protocol* type.
5. For the *Ping Interval*, enter the number of seconds to send ping requests.
6. For the *Failover Threshold*, enter the number of lost pings is acceptable before the port is determined to be down.
7. Select *OK*.

To add a ping server - CLI

```
config router gwdetect
  edit wan1
    set server <ISP_IP_address>
    set failtime <failure_count>
    set interval <seconds>
end
```

Routing

You need to configure a default route for each interface and indicate which route is preferred by specifying the distance. The lower distance is declared active and placed higher in the routing table.

When you have dual WAN interfaces that are configured to provide fail over, you might not be able to connect to the backup WAN interface because the FortiGate unit may not route traffic (even responses) out of the backup interface. The FortiGate unit performs a reverse path lookup to prevent spoofed traffic. If no entry can be found in the routing table which sends the return traffic out the same interface, then the incoming traffic is dropped.

To configure the routing of the two interfaces - web-based manager

1. Go to *Router* > *Static* > *Static Routes* and select *Create New*.

   For low-end FortiGate units, go to *System* > *Network* > *Routing* and select *Create New*.
2. Set the *Destination IP/Mask* to the address and netmask to 0.0.0.0/0.0.0.0.
3. Select the *Device* to the primary connection, *WAN1*.
4. Enter the *Gateway* address.
5. Select *Advanced*.
6. Set the *Distance* to `10`.
7. Select *OK*.
8. Repeat steps 1 through 7 setting the *Device* to *WAN2* and a *Distance* of `20`.

To configure the routing of the two interfaces - CLI

```
config router static
  edit 1
    set dst 0.0.0.0 0.0.0.0
    set device WAN1
    set gateway 0.0.0.0 0.0.0.0
    set distance 10
  next
  edit 1
    set dst <ISP_Address>
    set device WAN2
    set gateway <gateway_address>
    set distance 20
  next
end
```

Security policies

When creating security policies, you need to configure duplicate policies to ensure that after traffic fails over WAN1, regular traffic will be allowed to pass through WAN2 as it did with WAN1. This ensures that fail-over will occur with minimal affect to users. For more information on creating security policies see the *Firewall* Guide.

Load sharing

Load sharing enables you to use both connections to the internet at the same time, but do not provide fail over support. When configuring for load sharing, you need to ensure routing is configured for both external ports, for example, WAN1 and WAN2, have static routes with the same distance and priority.

Further configuration can be done using Equal Cost Multiple Path (ECMP). For more information on ECMP and load sharing, see the *Advanced Routing* Guide.

Link redundancy and load sharing

In this scenario, both links are available to distribute Internet traffic over both links. Should one of the interfaces fail, the FortiGate unit will continue to send traffic over the other active interface. Configuration is similar to the Redundant interfaces configuration, with the main difference being that the configured routes should have equal distance settings.

This means both routes will remain active in the routing table. To make one interface the preferred interface, use a default policy route to indicate the interface that is preferred for accessing the Internet. If traffic matches the security policy, the policy overrides all entries in the routing table, including connected routes. You may need to add a specific policy routes that override these default policy routes.

To redirect traffic over the secondary interface, create policy routes to direct some traffic onto it rather than the primary interface. When adding the policy route, only define the outgoing interface and leave the gateway blank. This ensures that the policy route will not be active when the link is down.

Single firewall vs. multiple virtual domains

A typical FortiGate setup, with a small to mid-range appliance, enables you to include a number of subnets on your network using the available ports and switch interfaces. This can potentially provide a means of having three or more mini networks for the various groups in a company. Within this infrastructure, multiple network administrators have access to the FortiGate to maintain security policies.

However, the FortiGate unit may not have enough interfaces to match the number of departments in the organization. If the FortiGate unit it running in transparent mode however, there is only one interface, and multiple network branches through the FortiGate are not possible.

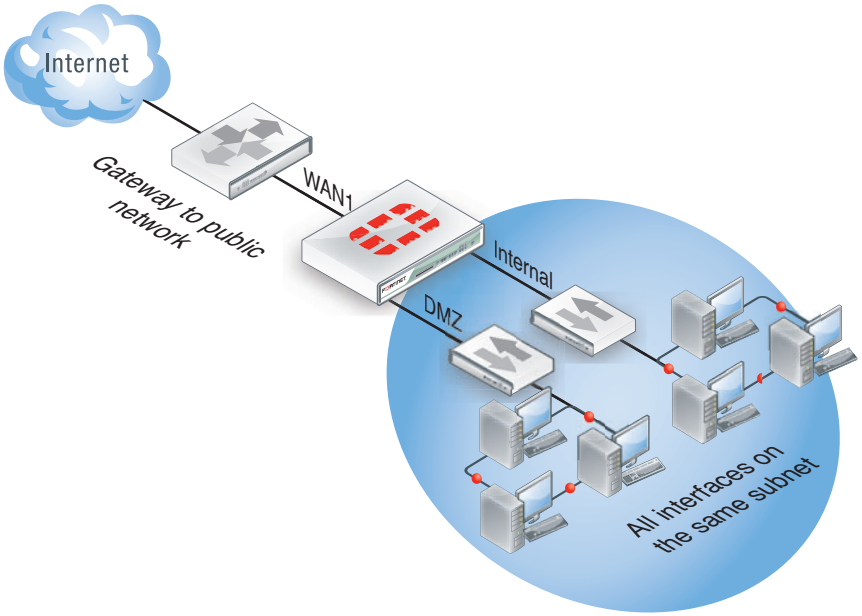
A FortiGate unit with Virtual Domains (VDOMs) enabled, provides a means to provide the same functionality in transparent mode as a FortiGate in NAT mode. VDOMs are a method of dividing a FortiGate unit into two or more virtual units that function as multiple independent units. VDOMs can provide separate security policies and, in NAT mode, completely separate configurations for routing and VPN services for each connected network. For administration, an administrator can be assigned to each VDOM, minimizing the possibility of error or fouling network communications.

By default, your FortiGate unit supports a maximum of 10 VDOMs. For select FortiGate models you can purchase a license key to increase the number of VODMs.

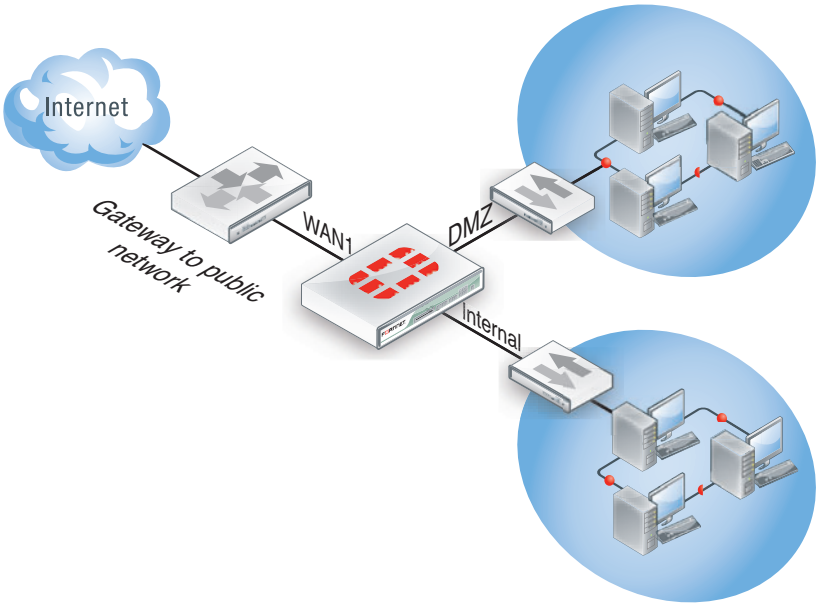
The FortiGate-20C and 30B and FortiWifi-20C and 30B do not support VDOMs.

Single firewall vs. vdoms

When VDOMs are not enabled, and the FortiGate unit is in transparent mode, all the interfaces on your unit become broadcast interfaces. The problem is there are no interfaces free for additional network segments.



A FortiGate with three interfaces means only limited network segments are possible without purchasing more FortiGate devices.



With multiple VDOMs you can have one of them configured in transparent mode, and the rest in NAT mode. In this configuration, you have an available transparent mode FortiGate unit you can drop into your network for troubleshooting, and you also have the standard.

This example shows how to enable VDOMs on the FortiGate unit and the basic and create a VDOM accounting on the DMZ2 port and assign an administrator to maintain the VDOM. First enable Virtual Domains on the FortiGate unit.

To enable VDOMs - web-based manager

1. Go to *System* > *Dashboard* > *Status*.
2. In the *System Information* widget, select *Enable* for *Virtual Domain.*

Note that on FortiGate-60 series and lower models, you need to enable VDOMs in the CLI only.

The FortiGate unit logs you out. Once you log back in, you will notice that the menu structure has changed. This reflects the global settings for all Virtual Domains.

To enable VDOMs - CLI

```
config system global
  set vdom-admin enable
end
```

Next, add the VDOM called accounting.

To add a VDOM - web-based manager

1. Go to *Global* > *VDOM* > *VDOM*, and select *Create New*.
2. Enter the VDOM name `accounting`.
3. Select *OK*.

To add a VDOM - CLI

```
config vdom
  edit <new_vdom_name>
end
```

With the Virtual Domain created, you can assign a physical interface to it, and assign it an IP address.

To assign physical interface to the accounting Virtual Domain - web-based manager

1. Go to *Global* > *Network* > *Interface*.
2. Select the DMZ2 port row and select *Edit*.
3. For the *Virtual Domain* drop-down list, select *accounting*.
4. Select the *Addressing Mode* of *Manual*.
5. Enter the IP address for the port of 10.13.101.100/24.
6. Set the *Administrative Access* to *HTTPS* and *SSH*.
7. Select *OK*.

To assign physical interface to the accounting Virtual Domain - CLI

```
config global
  config system interface
    edit dmz2
    set vdom accounting
    set ip 10.13.101.100/24
    set allowaccess https ssh
  next
end
```

Modem

FortiGate units support the use of wireless, 3G and 4G modems connected using the USB port or, if available, the express card slot. Modem access provides either primary or secondary (redundant) access to the Internet. For FortiGate units that do not include an internal modem (those units with an “M” designation), the modem interface will not appear in the web-based manager until enabled in the CLI. To enable the modem interface enter the CLI commands:

```
config system modem
  set status enable
end
```

You will need to log out of the FortiGate and log back in to see the modem configuration page at *System* > *Network* > *Modem*. Once enabled, modem options become available by going to *System* > *Network* > *Interface.*

Note that the modem interface is only available when the FortiGate unit is in NAT mode.

To configure modem settings, go to *System* > *Network* > *Modem*.

Configuring the modem settings is a matter of entering the ISP phone number, user name and password. Depending on the modem, additional information may need to be supplied such as product identifiers, and initialization strings.

The FortiGate unit includes a number of common modems within its internal database. You can view these by selecting the *Configure Modem* link on the *Modem Settings* page. If your modem is not on the list, select *Create New* to add the information. This information is stored on the device, and will remain after a reboot.

Fortinet has an online database of modem models and configuration settings through FortiGuard. A subscription to the FortiGuard services is not required to access the information. As models are added, you can select the *Configure Modem* link and select *Update Now* to download new configurations.

USB modem port

Each USB modem has a specific dial-out ttyusb port. This will be indicated with the documentation for your modem. To enable the correct USB port, use the CLI commands:

```
config system modem
  set wireless-port {ttyusb0 | ttyusb1 | ttyusb2}
end
```

To test the port, use the diagnose command:

```
diagnose sys modem com /ttyusb1
```

The ttyusb1 will be the value of your USB port selected. The response will be:

```
Serial port: /dev/ttyusb1
Press Ctrl+W to exit.
```

If the port does not respond the output will be:

```
Can not open modem device '/dev/ttyusb1' : Broken pipe
```

Modes

The FortiGate unit allows for two modes of operation for the modem; stand alone and redundant. In stand alone mode, the modem connects to a dialup ISP account to provide the connection to the Internet. In redundant mode, the modem acts as a backup method of connecting to the Internet, should the primary port for this function fails.

Configuring either stand alone or redundant modes are very similar. The primary difference is the selection of the interface that the modem will replace in the event of it failing, and the configuration of a PING server to monitor the chosen interface.

Configuring stand alone mode

Configuring stand alone mode is a matter of configuring the modem information and the dialing mode. The dial mode is either *Always Connect* or *Dial on demand*. Selecting *Always Connect* ensures that once the modem has connected, it remains connected to the ISP. Selecting *Dial on Demand*, the modem only calls the ISP if packets are routed to the modem interface. Once sent, the modem will disconnect after a specified amount of time.

To configure standalone mode as needed - web-based manager

1. Go to *System* > *Network* > *Modem*.
2. Select the *Mode* of *Standalone*.
3. Select the *Dial Mode* of *Dial on Demand*.
4. Enter the *Idle Timeout* of 2 minutes.
5. Select the number of redials the modem attempts if connection fails to 5.
6. Select *Apply*.

To configure standalone mode as needed- CLI

```
config system modem
  set mode standalone
  set auto-dial enable
  set idle-timer 2
  set redial 5
end
```

Configuring redundant mode

Redundant mode provides a backup to an interface, typically to the Internet. If that interface fails or disconnects, the modem automatically dials the configured phone number(s). Once connected, the FortiGate unit routes all traffic to the modem interface until the monitored interface is up again. The FortiGate unit pings the connection to determine when it is back online.

For the FortiGate to verify when the interface is back up, you need to configure a Ping server for that interface. You will also need to configure security policies between the modem interface and the other interfaces of the FortiGate unit to ensure traffic flow.

To configure redundant mode as needed - web-based manager

1. Go to *System* > *Network* > *Modem*.
2. Select the *Mode* of *Redundant*.
3. Select the interface the modem takes over from if it fails.
4. Select the *Dial Mode* of *Dial on Demand*.
5. Enter the *Idle Timeout* of 2 minutes.
6. Select the number of redials the modem attempts if connection fails to 5.
7. Select *Apply*.

To configure standalone mode as needed- CLI

```
config system modem
  set mode redundant
  set interface wan1
  set auto-dial enable
  set idle-timer 2
  set redial 5
end
```

Ping server

Adding a ping server is required for routing fail over traffic. A ping server will confirm the connectivity of the device's interface.

For low-end FortiGate units, go to *System* > *Admin* > *Settings* and enable *Dynamic Routing* before continuing.

To add a ping server - web-based manager

1. Go to *Router* > *Static* > *Settings* and select *Create New*.
2. Select the *Interface* that will send ping requests.
3. For the *Ping Server* field, enter the IP address of a server that the FortiGate unit will send ping requests to. This is typically a next hop router or gateway device.
4. Select the *Detect Protocol* type *ICMP Ping*.
5. For the *Ping Interval*, enter the number of seconds to send ping requests.
6. For the *Failover Threshold*, enter the number of lost pings is acceptable before the port is determined to be down.
7. Select *OK*.

To add a ping server - CLI

```
config router gwdetect
  edit wan1
    set server <ISP_IP_address>
    set failtime <failure_count>
    set interval <seconds>
end
```

Additional modem configuration

The CLI provides additional configuration options when setting up the modem options including adding multiple ISP dialing and initialization options and routing. For more information, see the *CLI Reference*.

Modem interface routing

The modem interface can be used in FortiOS as a dedicated interface. Once enabled and configured, you can use it in security policies and define static and dynamic routing. Within the CLI commands for the modem, you can configure the distance and priority of routes involving the modem interface. The CLI commands are:

```
config sysetm modem
  set distance <route_distance>
  set priority <priority_value>
end
```

For more information on the routing configuration in the CLI, see the *CLI Reference*. For more information on routing and configuring routing, see the *Advanced Routing* Guide.

DHCP servers and relays

Note that DHCP server options are not available in transparent mode.

A DHCP server provides an address to a client on the network, when requested, from a defined address range.

An interface cannot provide both a server and a relay for connections of the same type (regular or IPSec). However, you can configure a Regular DHCP server on an interface only if the interface is a physical interface with a static IP address. You can configure an IPSec DHCP server on an interface that has either a static or a dynamic IP address.

You can configure one or more DHCP servers on any FortiGate interface. A DHCP server dynamically assigns IP addresses to hosts on the network connected to the interface. The host computers must be configured to obtain their IP addresses using DHCP.

If an interface is connected to multiple networks via routers, you can add a DHCP server for each network. The IP range of each DHCP server must match the network address range. The routers must be configured for DHCP relay.

You can configure a FortiGate interface as a DHCP relay. The interface forwards DHCP requests from DHCP clients to an external DHCP server and returns the responses to the DHCP clients. The DHCP server must have appropriate routing so that its response packets to the DHCP clients arrive at the unit.

DHCP Server configuration

To add a DHCP server, go to *System* > *Network* > *Interface*. Edit the interface, and select *Enable* for the *DHCP Server* row.

DHCP Server IP	This appears only when *Mode* is *Relay*. Enter the IP address of the DHCP server where the FortiGate unit obtains the requested IP address.
Address Range	By default, the FortiGate unit assigns an address range based on the address of the interface for the complete scope of the address. For example, if the interface address is 172.20.120.230, the default range created is 172.20.120.231 to 172.20.120.254. Select the range and select *Edit* to adjust the range as needed, or select *Create New* to add a different range.
Netmask	Enter the netmask of the addresses that the DHCP server assigns.
Default Gateway	Select to either use the same IP as the interface or select *Specify* and enter the IP address of the default gateway that the DHCP server assigns to DHCP clients.
DNS Server	Select to use the system's DNS settings or select *Specify* and enter the IP address of the DNS server.
Advanced	
Mode	Select the type of DHCP server the FortiGate unit will be. By default, it is a server. Select *Relay* if needed. When *Relay* is selected, the above configuration is replaced by a field to enter the *DHCP Server IP* address.

Type	Select to use the DHCP in regular or IPsec mode.
MAC Address Access Control List	Select to match an IP address from the DHCP server to a specific client or device using its MAC address. In a typical situation, an IP address is assigned ad hoc to a client, and that assignment times out after a specific time of inactivity from the client, known as the lease time. To ensure a client or device always has the same IP address, that is, there is no lease time, use IP reservation. For more information, see "Assigning IP address by MAC address" on page 208.
Add from DHCP Client List	If the client is currently connected and using an IP address from the DHCP server, you can select this option to select the client from the list.

DHCP in IPv6

You can use DHCP with IPv6 using the CLI. To configure DHCP, ensure IPv6 is enabled by going to *System* > *Admin* > *Settings* and enable *IPv6*. Use the CLI command

```
config system dhcp6.
```

For more information on the configuration options, see the *CLI Reference*.

Service

On low-end FortiGate units, a DHCP server is configured, by default on the Internal interface:

IP Range	192.168.1.110 to 192.168.1.210
Netmask	255.255.255.0
Default gateway	192.168.1.99
Lease time	7 days
DNS Server 1	192.168.1.99

These settings are appropriate for the default Internal interface IP address of 192.168.1.99. If you change this address to a different network, you need to change the DHCP server settings to match.

Alternatively, after the FortiGate unit assigns an address, you can go to *System* > *Monitor* > *DHCP Monitor*, locate the particular user. Select the check box for the user and select *Add to Reserved*.

Lease time

The lease time determines the length of time an IP address remains assigned to a client. Once the lease expires, the address is released for allocation to the next client request for an IP

address The default lease time is seven days. To change the lease time, use the following CLI commands:

```
config system dhcp server
  edit <server_entry_number>
    set lease-time <seconds>
  end
```

To have an unlimited lease time, set the value to zero.

DHCP options

When adding a DHCP server, you have the ability to include DHCP codes and options. The DHCP options are BOOTP vendor information fields that provide additional vendor-independent configuration parameters to manage the DHCP server. For example, you may need to configure a FortiGate DHCP server that gives out a separate option as well as an IP address. For example, an environment that needs to support PXE boot with Windows images.

The option numbers and codes are specific to the particular application. The documentation for the application will indicate the values to use. Option codes are represented in a option value/HEX value pairs. The option is a value 1 and 255.

You can add up to three DHCP code/option pairs per DHCP server.

To configure option 252 with value http://192.168.1.1/wpad.dat - CLI

```
config system dhcp server
  edit <server_entry_number>
    set option1 252
        687474703a2f2f3139322e3136382e312e312f777061642e646174
end
```

For detailed information about DHCP options, see RFC 2132, DHCP Options and BOOTP Vendor Extensions.

Exclude addresses in DHCP a range

If you have a large address range for the DHCP server, you can block a range of addresses that will not be included in the available addresses for the connecting users. To do this, go to the CLI and enter the commands:

```
config system dhcp server
  edit <server_entry_number>
    config exclude-range
      edit <sequence_number>
        set start-ip <address>
        set end-ip <address>
      end
    end
  end
```

DHCP Monitor

To view information about DHCP server connections, go to *System* > *Monitor* > *DHCP Monitor*. On this page, you can also add IP address to the reserved IP address list.

Breaking a address lease

Should you need to end an IP address lease, you can break the lease using the CLI. This is useful if you have limited addresses, longer lease times where leases are no longer necessary. For example, with corporate visitors.

To break a lease enter the CLI command:

```
execute dhcp lease-clear <ip_address>
```

Assigning IP address by MAC address

To prevent users in the from changing their IP addresses and causing IP address conflicts or unauthorized use of IP addresses, you can bind an IP address to a specific MAC address using DHCP.

Use the CLI to reserve an IP address for a particular client identified by its device MAC address and type of connection. The DHCP server then always assigns the reserved IP address to the client. The number of reserved addresses that you can define ranges from 10 to 200 depending on the FortiGate model.

After setting up a DHCP server on an interface by going to *System* > *Network* > *Interface*, select the blue arrow next to *Advanced* to expand the options. If you know the MAC address of the system select *Create New* to add it, or if the system has already connected, locate it in the list, select its check box and select A*dd from DHCP Client List*.

You can also match an address to a MAC address in the CLI. In the example below, the IP address 10.10.10.55 for User1 is assigned to MAC address 00:09:0F:30:CA:4F.

```
config system dhcp reserved-address
  edit User1
    set ip 10.10.10.55
    set mac 00:09:0F:30:CA:4F
    set type regular
  end
```

DNS services

A DNS server is a public service that converts symbolic node names to IP addresses. A Domain Name System (DNS) server implements the protocol. In simple terms, it acts as a phone book for the Internet. A DNS server matches domain names with the computer IP address. This enables you to use readable locations, such as fortinet.com when browsing the Internet. FortiOS supports DNS configuration for both IPv4 and IPv6 addressing.

The FortiGate unit includes default DNS server addresses. However, these should be changed to those provided by your Internet Service Provider. The defaults are DNS proxies and are not as reliable as those from your ISP.

Within FortiOS, there are two DNS configuration options; each provide a specific service, and can work together to provide a complete DNS solution.

DNS settings

Basic DNS queries are configured on interfaces that connect to the Internet. When a web site is requested, for example, the FortiGate unit will look to the configured DNS servers to provide the IP address to know which server to contact to complete the transaction.

DNS server addresses are configured by going to *System* > *Network* > *DNS*. Here you specify the DNS server addresses. Typically, these addresses are supplied by your ISP. An additional option is available if you have local Microsoft domains on the network, by entering a domain name in the *Local Domain Name* field.

In a situation where all three fields are configured, the FortiGate unit will first look to the local domain. If no match is found, a request is sent to the external DNS servers.

If virtual domains are enabled, you create a DNS database in each VDOM. All of the interfaces in a VDOM share the DNS database in that VDOM.

Additional DNS CLI configuration

Further options are available from the CLI with the command `config system dns`. Within this command you can set the following commands:

- `dns-cache-limit` - enables you to set how many DNS entries are stored in the cache. Entries that remain in the cache provide a quicker response to requests than going out to the Internet to get the same information.
- `dns-cache-ttl` - enables you to set how long entries remain in the cache in seconds, between 60 and 86,400 (24 hours).
- `cache-notfound-responses` - when enabled, any DNS requests that are returned with NOTFOUND can be stored in the cache.
- `source-ip` - enables you to define a dedicated IP address for communications with the DNS server.

DNS server

You can also create local DNS servers for your network. Depending on your requirements, you can manually maintain your entries (master DNS server), or use it as a jumping point, where the server refers to an outside source (slave DNS server). A local master DNS server works similarly to the DNS server addresses configured in *System* > *Network* > *DNS*, but all entries must be added manually. This enables you to add a local DNS server to include specific URL/IP address combinations.

The DNS server options are not visible in the web-based manager by default. To enable the server, go to *System* > *Admin* > *Settings* and select *DNS Database.*

While a master DNS server is an easy method of including regularly used addresses to save on going to an outside DNS server, it is not recommended to make it the authoritative DNS server. IP addresses may change, and maintaining any type of list can quickly become labor-intensive.

A FortiGate master DNS server is best set for local services. For example, if your company has a web server on the DMZ that is accessed by internal employees as well as external users, such as customers or remote users. In this situation, the internal users when accessing the site would send a request for website.example.com, that would go out to the DNS server on the web, to return an IP address or virtual IP. With an internal DNS, the same site request is resolved internally to the internal web server IP address, minimizing inbound/outbound traffic and access time.

As a slave, DNS server, the FortiGate server refers to an external or alternate source as way to obtain the url/IP combination. This useful if there is a master DNS server for a large company where a list is maintained. Satellite offices can then connect to the master DNS server to obtain the correct addressing.

The DNS server entries does not allow CNAME entries, as per rfc 1912, section 2.4.

To configure a master DNS server - web-based manager

1. Go to *System* > *Network* > *DNS Server*, and select *Create New*.
2. Select the *Type* of *Master*.
3. Select the *View* as *Shadow*.
4. The view is the accessibility of the DNS server. Selecting *Public*, external users can access, or use, the DNS server. Selecting *Shadow*, only internal users can use it.
5. Enter the DNS *Zone*, for example, `WebServer`.
6. Enter the domain name for the zone, for example `example.com`.
7. Enter the hostname of the DNS server, for example, `Corporate`.
8. Enter the contact address for the administrator, for example, `admin@example.com`.
9. Set *Authoritative* to *Disable*.
10. Select *OK*.
11. Enter the DNS entries for the server by selecting *Create New*.
12. Select the *Type*, for example, *Address (A)*.
13. Enter the *Hostname*, for example `web.example.com`.
14. Enter the remaining information, which varies depending on the *Type* selected.
15. Select *OK*.

To configure a DNS server - CLI

```
config system dns-database
  edit WebServer
    set domain example.com
    set type master
    set view shadow
    set ttl 86400
    set primary-name corporate
    set contact admin@exmple.com
    set authoritative disable
      config dns-entry
        edit 1
          set hostname web.example.com
          set type A
          set ip 192.168.21.12
          set status enable
      end
    end
end
```

Recursive DNS

You can set an option to ensure these types of DNS server is not the authoritative server. When configured, the FortiGate unit will check its internal DNS server (Master or Slave). If the request cannot be fulfilled, it will look to the external DNS servers. This is known as a split DNS configuration.

You can also have the FortiGate unit look to an internal server should the Master or Slave not fulfill the request by using the CLI commands:

```
config system dns-database
  edit example.com
    ...
    set view shadow
end
```

For this behavior to work completely, for the external port, you must set the DNS query for the external interface to be recursive. This option is configured in the CLI only.

To set the DNS query

```
config system dns-server
  edit wan1
    set mode recursive
end
```

Dynamic DNS

If your ISP changes the your external IP address on a regular basis, and you have a static domain name, you can configure the external interface to use a dynamic DNS service to ensure external users and/or customers can always connect to your company firewall.

If you have a FortiGuard subscription, you can use FortiGuard as your DDNS server. To configure dynamic DNS in the web-based manager, go to *System* > *Network* > *DNS*, select *Enable FortiGuard DDNS*, and enter the relevant information for the interface communicating to the server, and which server to use, and relevant information.

If you do not have a FortiGuard subscription, or want to use an alternate server, you can configure dynamic DNS in the CLI use the commands below. Within the CLI you can configure a DDNS for each interface. Only the first configured port appears in the web-based manager. Additional commands vary with the DDNS server you select.

```
config system ddns
  edit <instance_value>
    set monitor-interface <external_interface>
    set ddns-server <ddns_server_selection>
end
```

You can also use FortiGuard (when subscribed) as a DDNS as well. To configure, use the CLI commands:

```
config system fortiguard
  set ddns-server-ip
  set ddns-server-port
end
```

FortiClient discovery and registration

FortiOS provides a means of allowing users running FortiClient Endpoint Control software to connect to specific interfaces when connecting to the FortiGate unit. As well as ensuring that remote or local users have FortiClient Endpoint Control software installed on their PC or mobile device.

FortiClient discovery

You can configure a FortiGate interface as an interface that will accept FortiClient connections. When configured, the FortiGate unit sends broadcast messages which the FortiClient software running on a end user PC is listening for.

To enable the broadcast message

1. Go to *System* > *Network* > *Interface*.
2. Edit the interface to send the broadcast messages.
3. Select *FCT-Access*.
4. In *Device Management*, select *Broadcast Discovery Messages*.
5. Select *OK*.

Once enabled, the FortiGate unit broadcasts a discovery message that includes the IP address of the interface and listening port number to the local network. All PCs running FortiClient on that network listen for this discovery message.

You also have the option of including a registration key. When the FortiClient discovers the FortiGate unit, it is prompted to enter a registration key, defined by the administrator.

To add a registration key

1. Go to *System* > *Config* > *Advanced*.
2. Select *Enable Registration Key for FortiClient*, and enter the key.
3. Select *Apply*.

Ensure you distribute the key to the users that need to connect to the FortiGate unit.

FortiClient Registration

On the end user side, if FortiClient has not been registered with the FortiGate unit, it is continually listening for the FortiGate discovery message. When this message is detected the un-registered client will pop-up a FortiGate Detected message. The user can choose to either register or ignore the message.

Clients that have registered with that FortiGate unit will not be listening for these messages and will not display the message again.

If you enabled the registration key, the user is prompted to enter the key before a connection can be completed.

For more information on FortiGate registration, see the *FortiClient Administration Guide*.

IP addresses for self-originated traffic

On the FortiGate unit, there are a number of protocols and traffic that is specific to the internal workings of FortiOS. For many of these traffic sources, you can identify a specific port/IP

address for this self-originating traffic. The following traffic can be configured to a specific port/IP address:

- SNMP
- Syslog
- alert email
- FortiManager connection IP
- FortiGuard services
- FortiAnalyzer logging
- NTP
- DNS
- Authorization requests such as RADIUS
- FSAE

Configuration of these services is performed in the CLI. In each instance, there is a command set `source-ip`. For example, to set the source IP of NTP to be on the DMZ1 port with an IP of 192.168.4.5, the commands are:

```
config system ntp
  set ntpsyn enable
  set syncinterval 5
  set source-ip 192.168.4.5
end
```

To see which services are configured with source-ip settings, use the get command:

```
get system source-ip status
```

The output will appear similar to the sample below:

```
NTP: x.x.x.x
DNS: x.x.x.x
SNMP: x.x.x.x
Central Management: x.x.x.x
FortiGuard Updates (AV/IPS): x.x.x.x
FortiGuard Queries (WebFilter/SpamFilter): x.x.x.x
```

Administration for schools

For system administrator in the school system it is particularly difficult to maintain a network and access to the Internet. There are potential legal liabilities if content is not properly filtered and children are allowed to view pornography and other non-productive and potentially dangerous content. For a school, too much filtering is better than too little. This section describes some basic practices administrators can employ to help maintain control without being too draconian for access to the internet.

Security policies

The default security policies in FortiOS allow all traffic on all ports and all IP addresses. Not the most secure. While applying UTM profiles can help to block viruses, detect attacks and prevent spam, this doesn't provide a solid overall security option. The best approach is a layered approach; the first layer being the security policy.

When creating outbound security policies, you need to know the answer to the question “What are the students allowed to do?” The answer is surf the web, connect to FTP sites, send/receive email, and so on.

Once you know what the students need to do, you can research the software used and determine the ports the applications use. For example, if the students only require web surfing, then there are only two ports (80 - HTTP and 443 - HTTPS) needed to complete their tasks. Setting the security policies to only allow traffic through two ports (rather than all 65,000), this will significantly lower any possible exploits. By restricting the ports to known services, mean s stopping the use of proxy servers, as many of them operate on a non-standard port to hide their traffic from URL filtering or HTTP inspection.

DNS

Students should not be allowed to use whatever DNS they want. this opens another port for them to use and potentially smuggle traffic on. The best approach is to point to an internal DNS server and only allow those devices out on port 53. Its the same approach one would use for SMTP. Only allow the mail server to use port 25 since nothing else should be sending email.

If there is no internal DNS server, then the list of allowed DNS servers they can use should be restrictive. One possible exploit would be for them to set up their own DNS server at home that serves different IPs for known hosts, such as having Google.com sent back the IP for playboy.com.

Encrypted traffic (HTTPS)

Generally speaking, students should not be allowed to access encrypted web sites. Encrypted traffic cannot be sniffed, and therefore, cannot be monitored. HTTPS traffic should only be allowed when necessary. Most web sites a student needs to access are HTTP, not HTTPS. Due to the nature of HTTPS protocol, and the fact that encryption is an inherent security risk to your network, its use should be restricted.

Adding a security policy that encompasses a list of allowed secure sites will ensure that any HTTPS sites that are required are the only sites a student can go to.

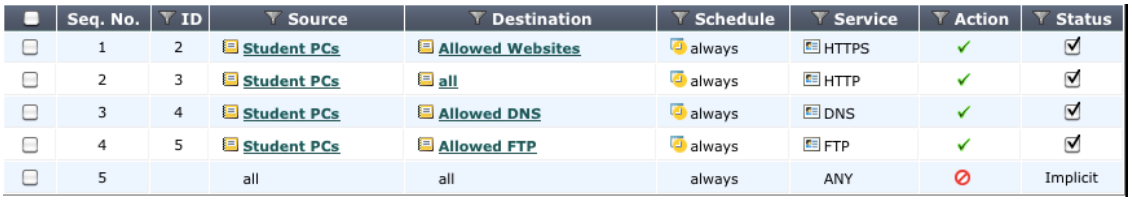
FTP

For the most part, students should not be using FTP. FTP is not HTTP or HTTPS so you cannot use URL flitting to restrict where they go. This can be controlled with destination IPs in the security policy. With a policy that specifically outlines which FTP addresses are allowed, all other will be blocked.

Example security policies

Given these requirements, an example set of security policies could look like the following illustration. In a large setup, all the IPs for the students are treated by one of these four policies.

Figure 24: Simple security policy setup



	Seq. No.	ID	Source	Destination	Schedule	Service	Action	Status
☐	1	2	Student PCs	Allowed Websites	always	HTTPS	✓	☑
☐	2	3	Student PCs	all	always	HTTP	✓	☑
☐	3	4	Student PCs	Allowed DNS	always	DNS	✓	☑
☐	4	5	Student PCs	Allowed FTP	always	FTP	✓	☑
☐	5		all	all	always	ANY	⊘	Implicit

The last policy in the list, included by default, is a deny policy.This adds to the potential of error that could end up allowing unwanted traffic to pass. The deny policy ensures that any traffic making it to this point is stopped. It can also help in further troubleshooting by viewing the logs for denied traffic.

With these policies in place, even before packet inspection occurs, the FortiGate, and the network are fairly secure. Should any of the UTM profiles fail, there is still a basic level of security.

UTM security profiles

Antivirus profiles

Antivirus screening should be enabled for any service you have enabled in the security policies. In the case above, HTTP, FTP, as well as POP3 and SMTP (assuming there is email access for students). There is not a virus scan option for HTTPS, because the content is encrypted. Generally speaking, most of the network traffic will be students surfing the web.

To configure antivirus profiles in the web-based manager, go to *UTM Security Profiles* > *Antivirus* > *Profile*, or use the CLI commands under `config antivirus profile`.

Web filtering

The actual filtering of URLs - sites and content - should be performed by FortiGuard. It is easier and web sites are constantly being monitored, and new ones reviewed and added to the FortiGuard databases every day. The FortiGuard categories provide an extensive list of offensive, and non-productive sites.

As well, there are additional settings to include in a web filtering profile to best contain a student's web browsing.

- Web URL filtering should be enabled to set up exemptions for web sites that are blocked or reasons other than category filtering. It also prevents the us of IP addresses to get around web filtering.
- Block invalid URLs - HTTPS only. This option inspects the HTTPS certificate and looks at the URL to ensure it's valid. It is common for proxy sites to create an HTTPS certificate with a garbage URL. If the site is legitimate, it should be set up correctly. If the site approach to security is to ignore it, then their security policy puts your network at risk and the site should be blocked.

Web filtering options are configured in the web-based manager by going to *UTM Security Profiles* > *Web filter* > *Profile*, or in the CLI under `config webfilter profile`.

Advanced options

There are a few Advanced options to consider for a web filtering profile:

- Enable *Provide details for blocked HTTP 4xx and 5xx errors*. Under normal circumstances there are exploits that can be used with 400 and 500 series messages to access the web

site. While most students probably won't know how to do this, there is no harm in being cautious. It only takes one.

- Enable *Rate Images by URL*. This option only works with Google images. It examines the URL that the images is stored at to get a rating on it, then blocks or allows the image based on the rating of the originating URL. It does not inspect the image contents. Most image search engines to a prefect and pass the images directly to the browser.
- Enable *Block HTTP redirects by rating*. An HTTP redirect is one method of getting around ratings. Go to one web site that has an allowed rating, and it redirects to another web site that may want blocked.

Categories and Classifications

For the selection of what FortiGuard categories and classifications that should be blocked, that is purely based on the school system and its Internet information policy.

Email Filtering

Other than specific teacher-led email inboxes, there is no reason why a student should be able to access, read or send personal email. Ports for POP3, SMTP and IMAP should not be opened in a security policies.

IPS

The intrusion protection profiles should be used to ensure the student PCs are not vulnerable to attacks, nor do you want students making attacks. As well, IPS can do more than simple vulnerability scans. With a FortiGuard subscription, IPS signatures are pushed to the FortiGate unit. New signatures are released constantly for various intrusions as they are discovered.

FortiOS includes a number of predefined IPS sensors that you can enable by default. Selecting the all_default signature is a good place to start as it includes the major signatures.

To configure IPS sensors in the web-based manager, go to *UTM Security Profiles* > *Intrusion Protection* > *IPS Sensor*, on the CLI use commands under `config ips sensor`.

Application control

Application control uses IPS signatures to limit the use of instant messaging and peer-to-peer applications which can lead to possible infections on a student's PC. FortiOS includes a number of pre-defined application categories. To configure and maintain application control profiles in the web-based manager, go to *UTM Security Profiles* > *Application Control* > *Application Sensor*. In the CLI use commands under `config application list`.

Some applications to consider include proxies, botnets, toolbars and P2P applications.

Logging

Turn on all logging - every option in this section should be enabled. This is not where you decide what you are going to log. It is simply defining what the UTM profiles can log.

Logging everything is a way to monitor traffic on the network, see what student's are utilizing the most, and locate any potential holes in your security plan. As well, keeping this information may help to prove negligence later in necessary.

Tag management

Tag management provide a method of categorizing, or labelling objects within FortiOS using keywords. You can give the following elements a “tag”, similar to a keyword:

- IPS signature
- application signature
- security policy
- firewall address

Tagging is way to organize the various elements, especially if you have a large number of addresses, security policies to manage and keep track of. Tagging enables you to break these elements into groups, but each element can belong to more than one group. Tags help you find elements which have something in common, be it a group, user or location. This is very similar to tagging found on photo sharing sites.

To use tagging, you need to enable it for 1U FortiGate units. It is enabled by default on all 2U FortiGate units and blades.

To enable tagging - web-based manager

1. Go to *System* > *Admin* > *Settings*.
2. Select *Object Tagging and Coloring*.
3. Select *Apply*.

To enable tagging - CLI

```
config system global
  set gui-object-tags enable
end
```

Adding and removing tags

You add and remove tags when you create the various elements. For example, when adding a firewall address, a section below the Interface selection enables you to add tags for that element, such as the department, region, or really, anything to help identify the element. When editing, applied tags appear as well. To add a tag, right-click on the element you want to add a tag to.

Figure 25: Adding tags to a new address.

To remove a tag, in the element, click the tag in the Applied Tags list.

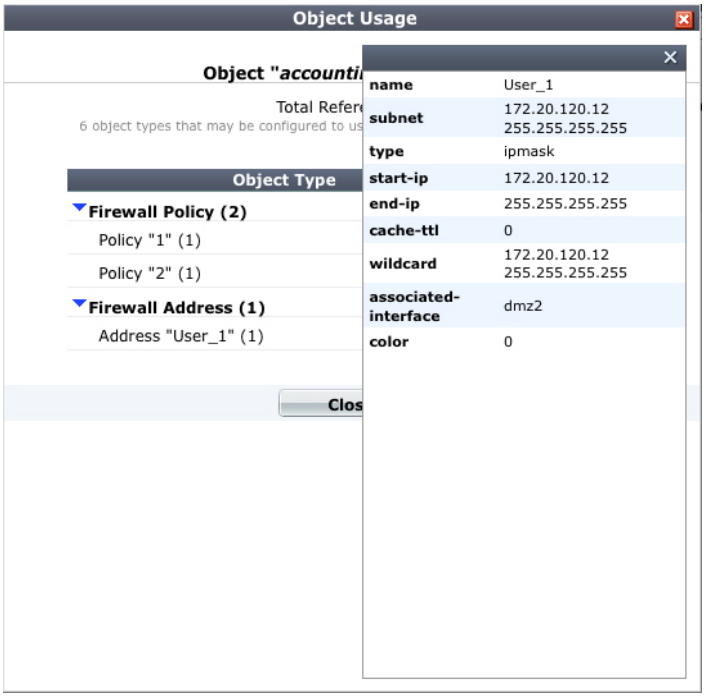
Reviewing tags

Tags can be reviewed in one location by going to *System* > *Config* > *Tag Management*. In this screen, all tags used appear. The visual size of the tag name indicates the usage; the bigger the size, the more it is used. By hovering over the keyword, a fly out indicates how many times it has been used.

To see where it was used, click the keyword. An *Object Usage* window displays all the reference categories where the keyword was used, and the number of times. Selecting the expand arrow further details its use.

Further, for security policies for example, you can select the *View* icon and see the details of the particular element. If need be, select the *Edit* icon to modify the element.

Figure 26: Viewing the address information for a tagged object



Tagging guidelines

Given the ease that tags can be added to elements in FortiOS, it makes sense to jump right in and begin applying tags to elements and object. However, this type of methodology will lead to problems down the road as new elements are added.

A methodology should be considered and developed before applying tags. This doesn't mean you need to develop an entire thesaurus or reference guide for all possibilities of tags. However, taking some time to develop a methodology for the keywords you intend to use will benefit later when new security policies, addresses, and so on are added. Some things to consider when developing a tag list:

- the hierarchy used for the organization such as region, city location, building location
- department names and if short forms or long forms are used
- will acronyms be used or terms spelled out.
- how granular will the tagging be

As tags are added, previously used tags appear so there is an opportunity to use previously used tags. However, you want to avoid a situation where both accounting and acct are both

options. This is also important if there are multiple administrators in different locations to ensure consistency.

At any time, you can change or even remove tags. It is best to do a bit of planning ahead of time to avoid unnecessary work later on.

Replacement messages list

The replacement message list in *System* > *Config* > *Replacement Messages*.

The replacement messages list enables you to view and customize replacement messages. Use the expand arrow beside each type to display the replacement messages for that category. Select the *Edit* icon beside each replacement message to customize that message for your requirements.

Should you make a major error to the code, you can select the *Restore Default* to return to the original message and code base.

If you are viewing the replacement messages list in a VDOM, any messages that have been customized for that VDOM are displayed with a Reset icon that you can use to reset the replacement message to the global version.

For connections requiring authentication, the FortiGate unit uses HTTP to send an authentication disclaimer page for the user to accept before a security policy is in effect. Therefore, the user must initiate HTTP traffic first in order to trigger the authentication disclaimer page. Once the disclaimer is accepted, the user can send whatever traffic is allowed by the security policy.

Replacement message images

You can add images to replacement messages to:

- disclaimer pages
- login pages
- declined disclaimer pages
- login failed page
- login challenge pages
- keepalive pages

Image embedding is also available to the endpoint NAC download portal and recommendation portal replacement messages, as well as HTTP replacement messages.

Supported image formats are GIF, JPEG, TIFF and PNG. The maximum file size supported is 6000 bytes.

Adding images to replacement messages

To upload an image for use in a message

1. Go to *System* > *Config* > *Replacement Messages*.
2. Select *Manage Images* at the top of the page.
3. Select *Create New*.
4. Enter a *Name* for the image.
5. Select the *Content Type*.
6. Select *Browse* to locate the file and select *OK*.

The image that you include in a replacement message, must have the following html:

```
<img src=%%IMAGE: <config_image_name>%% size=<bytes> >
```

For example:

```
<img src=%%IMAGE: logo_hq%% size=4272>
```

Modifying replacement messages

Replacement messages can be modified to include a message or content that suits your organization.

Use the expand arrows to view the replacement message list for a given category. Messages are in HTML format. For descriptions of the replacement message tags, see Replacement message tags.

To change a replacement message, go to *System* > *Config* > *Replacement Messages* select the replacement message that you want to modify. At the bottom pane of the window, you can the message on one side and the HTML code on the other side. The message view changes in real-time as you change the content.

A list of common replacement messages appears in the main window. To see the entire list and all categories of replacement messages, in the upper-right corner of the window, select *Extended View*.

Replacement message tags

Replacement messages can include replacement message tags, or variables. When users receive the message, the message tag is replaced with content relevant to the message. The table lists the replacement message tags that you can use.

Table 11: Replacement message tags

Tag	Description
%%AUTH_LOGOUT%%	The URL that will immediately delete the current policy and close the session. Used on the auth-keepalive page.
%%AUTH_REDIR_URL%%	The auth-keepalive page can prompt the user to open a new window which links to this tag.
%%CATEGORY%%	The name of the content category of the web site.
%%DEST_IP%%	The IP address of the request destination from which a virus was received. For email this is the IP address of the email server that sent the email containing the virus. This tag only works with alert email replacement messages.
%%DURATION%% (FortioS Carrier only)	The amount of time in the reporting period. This is user defined in the protection profile.
%%EMAIL_FROM%%	The email address of the sender of the message from which the file was removed.
%%EMAIL_TO%%	The email address of the intended receiver of the message from which the file was removed.
%%FAILED_MESSAGE%%	The failed to login message displayed on the auth-login-failed page.

Table 11: Replacement message tags (continued)

Tag	Description
%%FILE%%	The name of a file that has been removed from a content stream. This could be a file that contained a virus or was blocked by antivirus file blocking. %%FILE%% can be used in virus and file block messages.
%%FORTIGUARD_WF%%	The FortiGuard - Web Filtering logo.
%%FORTINET%%	The Fortinet logo.
%%LINK%%	The link to the FortiClient Host Security installs download for the Endpoint Control feature.
%%HTTP_ERR_CODE%%	The HTTP error code. “404” for example.
%%HTTP_ERR_DESC%%	The HTTP error description.
%%KEEPALIVEURL%% (FortiOS Carrier only)	auth-keepalive-page automatically connects to this URL every %%TIMEOUT%% seconds to renew the connection policy.
%%MMS_SENDER%% (FortiOS Carrier only)	Senders MSISDN from message header.
%%MMS_RECIPIENT%% (FortiOS Carrier only)	Recipients MSISDN from message header.
%%MMS_SUBJECT%% (FortiOS Carrier only)	MMS Subject line to help with message identity.
%%MMS_HASH_CHECKSUM%%	Value derived from hash calculation - will only be shown on duplicate message alerts.
%%MMS_THRESH%%	Mass MMS alert threshold that triggered this alert.
%%NIDSEVENT%%	The IPS attack message. %%NIDSEVENT%% is added to alert email intrusion messages.
%%NUM_MSG%% (FortiOS Carrier only)	The number of time the device tried to send the message with banned content within the reporting period.
%%OVERRIDE%%	The link to the FortiGuard Web Filtering override form. This is visible only if the user belongs to a group that is permitted to create FortiGuard web filtering overrides.
%%OVRD_FORM%%	The FortiGuard web filter block override form. This tag must be present in the FortiGuard Web Filtering override form and should not be used in other replacement messages.

Table 11: Replacement message tags (continued)

Tag	Description
%%PROTOCOL%%	The protocol (http, ftp, pop3, imap, or smtp) in which a virus was detected. %%PROTOCOL%% is added to alert email virus messages.
%%QUARFILENAME%%	The name of a file that has been removed from a content stream and added to the quarantine. This could be a file that contained a virus or was blocked by antivirus file blocking. %%QUARFILENAME%% can be used in virus and file block messages. Quarantining is only available on FortiGate units with a local disk.
%%QUOTA_INFO%%	Display information about the traffic shaping quota setting that is blocking the user. Used in traffic quota control replacement messages.
%%QUESTION%%	Authentication challenge question on auth-challenge page. Prompt to enter username and password on auth-login page.
%%SERVICE%%	The name of the web filtering service.
%%SOURCE_IP%%	The IP address of the request originator who would have received the blocked file. For email this is the IP address of the user's computer that attempted to download the message from which the file was removed. This tag only works with alert email replacement messages.
%%TIMEOUT%%	Configured number of seconds between authentication keepalive connections. Used on the auth-keepalive page.
%%URL%%	The URL of a web page. This can be a web page that is blocked by web filter content or URL blocking. %%URL%% can also be used in http virus and file block messages to be the URL of the web page from which a user attempted to download a file that is blocked.
%%VIRUS%%	The name of a virus that was found in a file by the antivirus system. %%VIRUS%% can be used in virus messages

Administration replacement message

If you enter the following CLI command the FortiGate unit displays the *Administration Login Disclaimer* whenever an administrator logs into the FortiGate unit's web-based manager or CLI.

```
config system global
  set access-banner enable
end
```

The web-based manager administrator login disclaimer contains the text of the Login Disclaimer replacement message as well as Accept and Decline buttons. The administrator must select accept to login.

Alert Mail replacement messages

The FortiGate unit adds the alert mail replacement messages listed in the following table to alert email messages sent to administrators. If you enable the option *Send alert email for logs based on severity*, whether or not replacement messages are sent by alert email depends on how you set the alert email in *Minimum log level*.

Authentication replacement messages

The FortiGate unit uses the text of the authentication replacement messages for various user authentication HTML pages that are displayed when a user is required to authenticate because a security policy includes at least one identity-based policy that requires firewall users to authenticate.

These replacement message pages are for authentication using HTTP and HTTPS. You cannot customize the firewall authentication messages for FTP and Telnet.

The authentication login page and the authentication disclaimer include replacement tags and controls not found on other replacement messages.

Users see the authentication login page when they use a VPN or a security policy that requires authentication. You can customize this page in the same way as you modify other replacement messages.

There are some unique requirements for these replacement messages:

- The login page must be an HTML page containing a form with `ACTION="/"` and `METHOD="POST"`
- The form must contain the following hidden controls:
  - `<INPUT TYPE="hidden" NAME="%%MAGICID%%" VALUE="%%MAGICVAL%%">`
  - `<INPUT TYPE="hidden" NAME="%%STATEID%%" VALUE="%%STATEVAL%%">`
  - `<INPUT TYPE="hidden" NAME="%%REDIRID%%" VALUE="%%PROTURI%%">`
- The form must contain the following visible controls:
  - `<INPUT TYPE="text" NAME="%%USERNAMEID%%" size=25>`
  - `<INPUT TYPE="password" NAME="%%PASSWORDID%%" size=25>`

Example

The following is an example of a simple authentication page that meets the requirements listed above.

```
<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD>
     <BODY><H4>You must authenticate to use this service.</H4>
<FORM ACTION="/" method="post">
     <INPUT NAME="%%MAGICID%%" VALUE="%%MAGICVAL%%" TYPE="hidden">
<TABLE ALIGN="center" BGCOLOR="#00cccc" BORDER="0"
     CELLPADDING="15" CELLSPACING="0" WIDTH="320"><TBODY>
<TR><TH>Username:</TH>
     <TD><INPUT NAME="%%USERNAMEID%%" SIZE="25" TYPE="text"> </TD></TR>
<TR><TH>Password:</TH>
     <TD><INPUT NAME="%%PASSWORDID%%" SIZE="25" TYPE="password">
     </TD></TR>
<TR><TD COLSPAN="2" ALIGN="center" BGCOLOR="#00cccc">
     <INPUT NAME="%%STATEID%%" VALUE="%%STATEVAL%%" TYPE="hidden">
```

```
    <INPUT NAME="%%REDIRID%%" VALUE="%%PROTURI%%" TYPE="hidden">
    <INPUT VALUE="Continue" TYPE="submit"> </TD></TR>
</TBODY></TABLE></FORM></BODY></HTML>
```

Captive Portal Default replacement messages

The Captive Portal Default replacement messages are used for wireless authentication only. You must have a VAP interface with the security set as captive portal to trigger these replacement messages.

Device Detection Portal replacement message

The FortiGate unit displays the replacement message when the FortiGate unit cannot determine the type of BYOD or handheld device is used to connect the network.

Email replacement messages

The FortiGate unit sends the mail replacement messages to email clients using IMAP, POP3, or SMTP when an event occurs such as antivirus blocking a file attached to an email that contains a virus. Email replacement messages are text messages.

If the FortiGate unit supports SSL content scanning and inspection these replacement messages can also be added to IMAPS, POP3S, and SMTPS email messages.

Endpoint Control replacement message

The FortiGate unit displays the replacement message when the FortiClient Endpoint Security software is not installed or registered correctly with the FortiGate unit.

FTP replacement messages

The FortiGate unit sends the FTP replacement messages listed in the table below to FTP clients when an event occurs such as antivirus blocking a file that contains a virus in an FTP session. FTP replacement messages are text messages.

FortiGuard Web Filtering replacement messages

The FortiGate unit sends the FortiGuard Web Filtering replacement messages listed in the table to web browsers using the HTTP protocol when FortiGuard web filtering blocks a URL, provides details about blocked HTTP 4xx and 5xx errors, and for FortiGuard overrides. FortiGuard Web Filtering replacement messages are HTTP pages.

If the FortiGate unit supports SSL content scanning and inspection and if *Protocol Recognition* > *HTTPS Content Filtering Mode* is set to Deep Scan in the antivirus profile, these replacement messages can also replace web pages downloaded using the HTTPS protocol.

HTTP replacement messages

The FortiGate unit sends the HTTP replacement messages listed in the following table to web browsers using the HTTP protocol when an event occurs such as antivirus blocking a file that contains a virus in an HTTP session. HTTP replacement messages are HTML pages.

If the FortiGate unit supports SSL content scanning and inspection, and if under HTTPS in the protocol option list has Enable Deep Scan enabled, these replacement messages can also replace web pages downloaded using the HTTPS protocol.

IM replacement messages

The FortiGate unit sends the IM replacement messages listed in to IM clients using AIM, ICQ, MSN, or Yahoo! Messenger when an event occurs such as antivirus blocking a file attached to an email that contains a virus. IM replacement messages are text messages.

NNTP replacement messages

The FortiGate unit sends the NNTP replacement messages listed in the following table to NNTP clients when an event occurs such as antivirus blocking a file attached to an NNTP message that contains a virus. NNTP replacement messages are text messages.

Spam replacement messages

The FortiGate unit adds the Spam replacement messages listed in the following table to SMTP server responses if the email message is identified as spam and the spam action is discard. If the FortiGate unit supports SSL content scanning and inspection these replacement messages can also be added to SMTPS server responses.

NAC quarantine replacement messages

The page that is displayed for the user depends on whether NAC quarantine blocked the user because a virus was found, a DoS sensor detected an attack, an IPS sensor detected an attack, or a DLP rule with action set to *Quarantine IP address* or *Quarantine Interface* matched a session from the user.

The default messages inform the user of why they are seeing this page and recommend they contact the system administrator. You can customize the pages as required, for example to include an email address or other contact information or if applicable a note about how long the user can expect to be blocked.

SSL VPN replacement message

The SSL VPN login replacement message is an HTML replacement message that formats the FortiGate SSL VPN portal login page. You can customize this replacement message according to your organization's needs. The page is linked to FortiGate functionality and you must construct it according to the following guidelines to ensure that it will work.

- The login page must be an HTML page containing a form with `ACTION="%%SSL_ACT%%" and METHOD="%%SSL_METHOD%%"`
- The form must contain the `%%SSL_LOGIN%%` tag to provide the login form.
- The form must contain the `%%SSL_HIDDEN%%` tag.

Web Proxy replacement messages

The FortiGate unit sends Web Proxy replacement messages listed in the table below when a web proxy event occurs that is detected and matches the web proxy configuration. These replacement messages are web pages that appear within your web browser.

The following web proxy replacement messages require an identity-based security policy so that the web proxy is successful. You can also enable FTP-over-HTTP by selecting the *FTP* option in *System* > *Network* > *Explicit Proxy*.

Traffic quota control replacement messages

When user traffic is going through the FortiGate unit and it is blocked by traffic shaping quota controls, users see the *Traffic shaper block message* or the *Per IP traffic shaper block message* when they attempt to connect through the FortiGate unit using HTTP.

The traffic quota HTTP pages should contain the `%%QUOTA_INFO%%` tag to display information about the traffic shaping quota setting that is blocking the user.

MM1 replacement messages

MM1 replacement messages are sent when, during MMS content scanning, FortiOS Carrier detects, for example a virus, using the MMS profile.

You must have *Remove Blocked* selected within the MMS profile if you want to remove the content that is intercepted during MMS scanning on the FortiGate unit.

MM3 replacement messages

MM3 replacement messages are sent when, during MMS content scanning, FortiOS Carrier detects, for example a virus, using the MMS profile.

You must have *Remove Blocked* selected within the MMS profile if you want to remove the content that is intercepted during MMS scanning on the unit.

MM4 replacement messages

MM4 replacement messages are sent when, during MMS content scanning, FortiOS Carrier detects, for example a virus, using the MMS profile.

MM7 replacement messages

MM7 replacement messages are sent when, during MMS content scanning, FortiOS Carrier detects, for example a virus, using the MMS profile.

MMS replacement messages

The MMS replacement message is sent when a section of an MMS message has been replaced because it contains a blocked file. This replacement message is in HTML format.

The message text is:

```
<HTML><BODY>This section of the message has been replaced because it
contained a blocked file</BODY></HTML>
```

Replacement message groups

Replacement message groups enable you to view common messages in groups for large carriers. To view grouped replacement messages, go to *System* > *Admin* > *Settings* and select *Replacement Message Groups* in the *Display Options on GUI* section.

Message groups can be configured by going to *Config* > *Replacement Message Group*.

Using the defined groups, you can manage specific replacement messages from a single location, rather than searching through the entire replacement message list.

If you enable virtual domains (VDOMs) on the FortiGate unit, replacement message groups are configured separately for each virtual domain. Each virtual domain has its own default

replacement message group, configured from *System* > *Config* > *Replacement Messages Group*.

When you modify a message in a replacement message group, a Reset icon appears beside the message in the group. You can select this Reset icon to reset the message in the replacement message group to the default version.

All MM1/4/7 notification messages for FortiOS Carrier (and MM1 retrieve-conf messages) can contain a SMIL layer and all MM4 notification messages can contain an HTML layer in the message. These layers can be used to brand messages by using logos uploaded to the FortiGate unit via the 'Manage Images' link found on the replacement message group configuration page.

Disk

To view the status and storage information of the local disk on your FortiGate unit, go to *System* > *Config* > *Advanced*. The *Disk* menu appears only on FortiGate units with an internal hard or flash disk.

Formatting the disk

The internal disk of the FortiGate unit (if available) can be formatted by going to *System* > *Config* > *Disk* and selecting *Format*.

Formatting the disk will erase all data on it, including databases for antivirus and IPS; logs, quarantine files, and WAN optimization caches. The FortiGate unit requires a reboot once the disk has been formatted.

Setting space quotas

If the FortiGate unit has an internal hard or flash disk, you can allocate the space on the disk for specific logging and archiving, and WAN optimization. By default, the space is used on an as required basis. As such, a disk can fill up with basic disk logging, leaving less potential space for quarantine.

By going to *System* > *Config* > *Disk*, you can select the *Edit* icon for *Logging and Archiving* and *WAN Optimization & Web Cache* and define the amount of space each log, archive and WAN optimization has on the disk.

CLI Scripts

To upload bulk CLI commands and scripts, go to *System* > *Config* > *Advanced*.

Scripts are text files containing CLI command sequences. Scripts can be used to deploy identical configurations to many devices. For example, if all of your devices use identical security policies, you can enter the commands required to create the security policies in a script, and then deploy the script to all the devices which should use those same settings.

Use a text editor such as Notepad or other application that creates simple text files. Enter the commands in sequence, with each line as one command, similar to examples throughout the FortiOS documentation set.

If you are using a FortiGate unit that is not remotely managed by a FortiManager unit or the FortiGuard Analysis and Management Service, the scripts you upload are executed and discarded. If you want to execute a script more than once, you must keep a copy on your management PC.

If your FortiGate unit is configured to use a FortiManager unit, you can upload your scripts to the FortiManager unit, and run them from any FortiGate unit configured to use the FortiManager unit. If you upload a script directly to a FortiGate unit, it is executed and discarded.

If your FortiGate unit is configured to use FortiGuard Analysis and Management Service, scripts you upload are executed and stored. You can run uploaded scripts from any FortiGate unit configured with your FortiGuard Analysis and Management Service account. The uploaded script files appear on the FortiGuard Analysis and Management Service portal web site.

Uploading script files

After you have created a script file, you can then upload it through *System* > *Config* > *Advanced*. When a script is uploaded, it is automatically executed.

Commands that require the FortiGate unit to reboot when entered in the command line will also force a reboot if included in a script.

To execute a script

1. Go to *System* > *Config* > *Advanced*.
2. Verify that *Upload Bulk CLI Command File* is selected.
3. Select *Browse* to locate the script file.
4. Select *Apply*.

If the FortiGate unit is not configured for remote management, or if it is configured to use a FortiManager unit, uploaded scripts are discarded after execution. Save script files to your management PC if you want to execute them again later.

If the FortiGate unit is configured to use the FortiGuard Analysis and Management Service, the script file is saved to the remote server for later reuse. You can view the script or run it from the FortiGuard Analysis and Management Service portal web site.

Rejecting PING requests

The factory default configuration of your FortiGate unit allows the default external interface to respond to ping requests. Depending on the model of your FortiGate unit the actual name of this interface will vary. For the most secure operation, you should change the configuration of the external interface so that it does not respond to ping requests. Not responding to ping requests makes it more difficult for a potential attacker to detect your FortiGate unit from the Internet. One such potential threat are Denial of Service (DoS) attacks.

A FortiGate unit responds to ping requests if ping administrative access is enabled for that interface.

To disable ping administrative access - web-based manager

1. Go to *System* > *Network* > *Interface*.
2. Choose the external interface and select *Edit*.
3. Clear the *Ping Administrative Access* check box.
4. Select *OK*.

In the CLI, when setting the allowaccess settings, by selecting the access types and not including the PING option, that option is then not selected. In this example, only HTTPS is selected.

To disable ping administrative access - CLI

```
config system interface
  edit external
    set allowaccess https
end
```

Opening TCP 113

Although seemingly contrary to conventional wisdom of closing ports from hackers, this port, which is used for ident requests, should be opened.

Port 113 initially was used as an authentication port, and later defined as an identification port (see RFC 1413). Some servers may still use this port to help in identifying users or other servers and establish a connection. Because port 113 receives a lot of unsolicited traffic, many routers, including on the FortiGate unit, close this port.

The issue arises in that unsolicited requests are stopped by the FortiGate unit, which will send a response saying that the port is closed. In doing so, it also lets the requesting server know there is a device at the given address, and thus announcing its presence. By enabling traffic on port 113, requests will travel to this port, and will most likely, be ignored and never responded to.

By default, the ident port is closed. To open it, use the following CLI commands:

```
config system interface
  edit <port_name>
    set ident_accept enable
end
```

You could also further use port forwarding to send the traffic to a non-existent IP address and thus never have a response packet sent.

Obfuscate HTTP responses

The FortiGate unit can obfuscate the HTTP responses from the FortiGate admin GUI and SSL VPN servers. By default this option is not enabled. To obfuscate HTTP headers, use the following CLI command:

```
config system global
  set http-obfucate {none | header-only | modified | no-error}
end
```

Where:

`none` — do not hide the FortiGate web server identity.

`header-only` — hides the HTTP server banner.

`modified` — provides modified error responses.

`no-error` — suppresses error responses.

Session helpers

The FortiOS firewall can analyze most TCP/IP protocol traffic by comparing packet header information to security policies. This comparison determines whether to accept or deny the packet and the session that the packet belongs to.

Some protocols include information in the packet body (or payload) that must be analyzed to successfully process sessions for this protocol. For example, the SIP VoIP protocol uses TCP control packets with a standard destination port to set up SIP calls. But the packets that carry the actual conversation can use a variety of UDP protocols with a variety of source and destination port numbers. The information about the protocols and port numbers used for a SIP call is contained in the body of the SIP TCP control packets. To successfully process SIP VoIP calls, FortiOS must be able to extract information from the body of the SIP packet and use this information to allow the voice-carrying packets through the firewall.

FortiOS uses session helpers to analyze the data in the packet bodies of some protocols and adjust the firewall to allow those protocols to send packets through the firewall.

This section includes the topics:

Viewing the session helper configuration

You can view the session helpers enabled on your FortiGate unit in the CLI using the commands below. The following output shows the first two session helpers. The number of session helpers can vary to around 20.

```
show system session-helper
  config system session-helper
    edit 1
      set name pptp
      set port 1723
      set protocol 6
```

```
    end
    next
      set name h323
      set port 1720
      set protocol 6
    next
    end
    .
    .
```

The configuration for each session helper includes the name of the session helper and the port and protocol number on which the session helper listens for sessions. Session helpers listed on protocol number 6 (TCP) or 17 (UDP). For a complete list of protocol numbers see: Assigned Internet Protocol Numbers.

For example, the output above shows that FortiOS listens for PPTP packets on TCP port 1723 and H.323 packets on port TCP port 1720.

If a session helper listens on more than one port or protocol the more than one entry for the session helper appears in the `config system session-helper` list. For example, the pmap session helper appears twice because it listens on TCP port 111 and UDP port 111. The rsh session helper appears twice because it listens on TCP ports 514 and 512.

Changing the session helper configuration

Normally you will not need to change the configuration of the session helpers. However in some cases you may need to change the protocol or port the session helper listens on.

Changing the protocol or port that a session helper listens on

Most session helpers are configured to listen for their sessions on the port and protocol that they typically use. If your FortiGate unit receives sessions that should be handled by a session helper on a non-standard port or protocol you can use the following procedure to change the port and protocol used by a session helper. The following example shows how to change the port that the pmap session helper listens on for Sun RPC portmapper TCP sessions. By default pmap listens on TCP port 111.

To change the port that the pmap session helper listens on to TCP port 112

1. Confirm that the TCP pmap session helper entry is 11 in the session-helper list:

```
show system session-helper 11
  config system session-helper
    edit 11
      set name pmap
      set port 111
      set protocol 6
    next
  end
```

2. Enter the following command to change the TCP port to 112.

```
config system session-helper
  edit 11
    set port 112
  end
```

3. The pmap session helper also listens on UDP port 111. Confirm that the UDP pmap session helper entry is 12 in the session-helper list:

```
show system session-helper 12
  config system session-helper
    edit 12
      set name pmap
      set port 111
      set protocol 17
    next
  end
```

4. Enter the following command to change the UDP port to 112.

```
config system session-helper
  edit 12
    set port 112
  end
end
```

Use the following command to set the h323 session helper to listen for ports on the UDP protocol.

To change the protocol that the h323 session helper listens on

1. Confirm that the h323 session helper entry is 2 in the session-helper list:

```
show system session-helper 2
  config system session-helper
    edit 2
      set name h323
      set port 1720
      set protocol 6
    next
  end
```

2. Enter the following command to change the protocol to UDP.

```
config system session-helper
  edit 2
    set protocol 17
  end
end
```

If a session helper listens on more than one port or protocol, then multiple entries for the session helper must be added to the session helper list, one for each port and protocol combination. For example, the rtsp session helper listens on TCP ports 554, 7070, and 8554 so there are three rtsp entries in the session-helper list. If your FortiGate unit receives rtsp packets on a different TCP port (for example, 6677) you can use the following command to configure the rtsp session helper to listen on TCP port 6677.

To configure a session helper to listen on a new port and protocol

```
config system session-helper
  edit 0
    set name rtsp
    set port 6677
    set protocol 6
end
```

Disabling a session helper

In some cases you may need to disable a session helper. Disabling a session helper just means removing it from the session-helper list so that the session helper is not listening on a port. You can completely disable a session helper by deleting all of its entries from the session helper list. If there are multiple entries for a session helper on the list you can delete one of the entries to prevent the session helper from listening on that port.

To disable the mgcp session helper from listening on UDP port 2427

1. Enter the following command to find the mgcp session helper entry that listens on UDP port 2427:

```
show system session-helper
   .
   .
   .
edit 19
   set name mgcp
   set port 2427
   set protocol 17
next
   .
   .
   .
```

2. Enter the following command to delete session-helper list entry number 19 to disable the mgcp session helper from listening on UDP port 2427:

```
config system session-helper
   delete 19
```

By default the mgcp session helper listens on UDP ports 2427 and 2727. The previous procedure shows how to disable the mgcp protocol from listening on port 2427. The following procedure completely disables the mgcp session helper by also disabling it from listening on UDP port 2727.

To completely disable the mgcp session helper

1. Enter the following command to find the mgcp session helper entry that listens on UDP port 2727:

```
show system session-helper
   .
   .
   .
edit 20
   set name mgcp
   set port 2727
   set protocol 17
next
   .
   .
   .
```

2. Enter the following command to delete session-helper list entry number 20 to disable the mgcp session helper from listening on UDP port 2727:

```
config system session-helper
   delete 20
```

DCE-RPC session helper (dcerpc)

Distributed Computing Environment Remote Procedure Call (DCE-RPC) provides a way for a program running on one host to call procedures in a program running on another host. DCE-RPC (also called MS RPC for Microsoft RPC) is similar to ONC-RPC. Because of the large number of RPC services, for example, MAPI, the transport address of an RPC service is dynamically negotiated based on the service program's universal unique identifier (UUID). The Endpoint Mapper (EPM) binding protocol in FortiOS maps the specific UUID to a transport address.

To accept DCE-RPC sessions you must add a security policy with service set to any or to the DEC-RPC pre-defined service (which listens on TCP and UDP ports 135). The dcerpc session helper also listens on TCP and UDP ports 135.

The session allows FortiOS to handle DCE-RPC dynamic transport address negotiation and to ensure UUID-based security policy enforcement. You can define a security policy to permit all RPC requests or to permit by specific UUID number.

In addition, because a TCP segment in a DCE-RPC stream might be fragmented, it might not include an intact RPC PDU. This fragmentation occurs in the RPC layer; so FortiOS does not support parsing fragmented packets.

DNS session helpers (dns-tcp and dns-udp)

FortiOS includes two DNS session helpers, dns-tcp, a session helper for DNS over TCP, and dns-udp, a session helper for DNS over UDP.

To accept DNS sessions you must add a security policy with service set to any or to the DNS pre-defined service (which listens on TCP and UDP ports 53). The dns-udp session helper also listens on UDP port 53. By default the dns-tcp session helper is disabled. If needed you can use the following command to enable the dns-tcp session helper to listen for DNS sessions on TCP port 53:

```
config system session-helper
  edit 0
    set name dns-tcp
    set port 53
    set protocol 6
end
```

File transfer protocol (FTP) session helper (ftp)

The FTP session helper monitors PORT, PASV and 227 commands and NATs the IP addresses and port numbers in the body of the FTP packets and opens ports on the FortiGate unit as required.

To accept FTP sessions you must add a security policy with service set to any or to the FTP, FTP_Put, and FTP_GET pre-defined services (which all listen on TCP port 21).

H.245 session helpers (h245I and h245O)

H.245 is a control channel protocol used for H.323 and other similar communication sessions. H.245 sessions transmit non-telephone signals. H.245 sessions carry information needed for multimedia communication, such as encryption, flow control jitter management and others.

FortiOS includes two H.245 sessions helpers, h245I which is for H.245 call in and h245O which is for H.245 call out sessions. There is no standard port for H.245. By default the H.245 sessions helpers are disabled. You can enable them as you would any other session helper. When you enable them, you should specify the port and protocol on which the FortiGate unit receives H.245 sessions.

H.323 and RAS session helpers (h323 and ras)

The H.323 session helper supports secure H.323 voice over IP (VoIP) sessions between terminal endpoints such as IP phones and multimedia devices. In H.323 VoIP networks, gatekeeper devices manage call registration, admission, and call status for VoIP calls. The FortiOS h323 session helper supports gatekeepers installed on two different networks or on the same network.

To accept H.323 sessions you must add a security policy with service set to any or to the H323 pre-defined service (which listens on TCP port numbers 1720 and 1503 and on UDP port number 1719). The h323 session helper listens on TCP port 1720.

The ras session helper is used with the h323 session helper for H.323 Registration, Admission, and Status (RAS) services. The ras session helper listens on UDP port 1719.

Alternate H.323 gatekeepers

The h323 session helper supports using H.323 alternate gatekeepers. All the H.323 end points must register with a gatekeeper through the Registration, Admission, and Status (RAS) protocol before they make calls. During the registration process, the primary gatekeeper sends Gatekeeper Confirm (GCF) and Registration Confirm (RCF) messages to the H.323 end points that contain the list of available alternate gatekeepers.

The alternate gatekeeper provides redundancy and scalability for the H.323 end points. If the primary gatekeeper fails the H.323 end points that have registered with that gatekeeper are automatically registered with the alternate gatekeeper. To use the H.323 alternate gatekeeper, you need to configure security policies that allow H.323 end points to reach the alternate gatekeeper.

Media Gateway Controller Protocol (MGCP) session helper (mgcp)

The Media Gateway Control Protocol (MGCP) is a text-based application layer protocol used for VoIP call setup and control. MGCP uses a master-slave call control architecture in which the media gateway controller uses a call agent to maintain call control intelligence, while the media gateways perform the instructions of the call agent.

To accept MGCP sessions you must add a security policy with service set to any or to the MGCP pre-defined service (which listens on UDP port numbers 2427 and 2727). The h323 session helper also listens on UDP port numbers 2427 and 2727.

The MGCP session helper does the following:

- VoIP signalling payload inspection. The payload of the incoming VoIP signalling packet is inspected and malformed packets are blocked.
- Signaling packet body inspection. The payload of the incoming MGCP signaling packet is inspected according to RFC 3435. Malformed packets are blocked.
- Stateful processing of MGCP sessions. State machines are invoked to process the parsed information. Any out-of-state or out-of-transaction packet is identified and properly handled.
- MGCP Network Address Translation (NAT). Embedded IP addresses and ports in packet bodies is properly translated based on current routing information and network topology, and is replaced with the translated IP address and port number, if necessary.
- Manages pinholes for VoIP traffic. To keep the VoIP network secure, the IP address and port information used for media or signalling is identified by the session helper, and pinholes are dynamically created and closed during call setup.

ONC-RPC portmapper session helper (pmap)

Open Network Computing Remote Procedure Call (ONC-RPC) is a widely deployed remote procedure call system. Also called Sun RPC, ONC-RPC allows a program running on one host to call a program running on another. The transport address of an ONC-RPC service is dynamically negotiated based on the service's program number and version number. Several binding protocols are defined for mapping the RPC program number and version number to a transport address.

To accept ONC-RPC sessions you must add a security policy with service set to any or to the ONC-RPC pre-defined service (which listens on TCP and UDP port number 111). The RPC portmapper session helper (called pmap) handles the dynamic transport address negotiation mechanisms of ONC-RPC.

PPTP session helper for PPTP traffic (pptp)

The PPTP session help supports port address translation (PAT) for PPTP traffic. PPTP provides IP security at the Network Layer. PPTP consists of a control session and a data tunnel. The control session runs over TCP and helps in establishing and disconnecting the data tunnel. The data tunnel handles encapsulated Point-to-Point Protocol (PPP) packets carried over IP.

To accept PPTP sessions that pass through the FortiGate unit you must add a security policy with service set to any or to the PPTP pre-defined service (which listens on IP port 47 and TCP port 1723). The pptp session helper listens on TCP port 1723.

PPTP uses TCP port 1723 for control sessions and Generic Routing Encapsulation (GRE) (IP protocol 47) for tunneling the encapsulated PPP data. The GRE traffic carries no port number, making it difficult to distinguish between two clients with the same public IP address. PPTP uses the source IP address and the Call ID field in the GRE header to identify a tunnel. When multiple clients sharing the same IP address establish tunnels with the same PPTP server, they may get the same Call ID. The call ID value can be translated in both the control message and the data traffic, but only when the client is in a private network and the server is in a public network.

PPTP clients can either directly connect to the Internet or dial into a network access server to reach the Internet. A FortiGate unit that protects PPTP clients can translate the clients' private IP addresses to a pool of public IP addresses using NAT port translation (NAT-PT). Because the GRE traffic carries no port number for address translation, the pptp session helper treats the Call ID field as a port number as a way of distinguishing multiple clients.

After the PPTP establishing a TCP connection with the PPTP server, the client sends a start control connection request message to establish a control connection. The server replies with a start control connection reply message. The client then sends a request to establish a call and sends an outgoing call request message. FortiOS assigns a Call ID (bytes 12-13 of the control message) that is unique to each PPTP tunnel. The server replies with an outgoing call reply message that carries its own Call ID in bytes 12-13 and the client's call ID in bytes 14-15. The pptp session helper parses the control connection messages for the Call ID to identify the call to which a specific PPP packet belongs. The session helper also identifies an outgoing call request message using the control message type field (bytes 8-9) with the value 7. When the session helper receives this message, it parses the control message for the call ID field (bytes 12-13). FortiOS translates the call ID so that it is unique across multiple calls from the same translated client IP. After receiving outgoing call response message, the session helper holds this message and opens a port that accepts GRE traffic that the PPTP server sends. An outgoing call request message contains the following parts:

- The protocol used for the outgoing call request message (usually GRE)
- Source IP address (PPTP server IP)
- Destination IP address (translated client IP)
- Destination port number (translated client call ID)

The session helper identifies an outgoing call reply message using the control message type field (bytes 8-9) with the value 8. The session helper parses these control messages for the call ID field (bytes 12-13) and the client's call ID (bytes 14-15). The session helper then uses the client's call ID value to find the mapping created for the other direction, and then opens a pinhole to accept the GRE traffic that the client sends.

An outgoing call reply message contains the following parts:

- Protocol used for the outgoing call reply message (usually GRE)
- Source IP address (PPTP client IP)
- Destination IP address (PPTP server IP)
- Destination port number (PPTP server Call ID)

Each port that the session opens creates a session for data traffic arriving in that direction. The session helper opens the following two data sessions for each tunnel:

- Traffic from the PPTP client to the server, using the server's call ID as the destination port
- Traffic from the PPTP server to the client, using the client's translated call ID as the destination port

The default timeout value of the control connection is 30 minutes. The session helper closes the pinhole when the data session exceeds the timeout value or is idle for an extended period.

Remote shell session helper (rsh)

Using the remote shell program (RSH), authenticated users can run shell commands on remote hosts. RSH sessions most often use TCP port 514. To accept RSH sessions you must add a security policy with service set to any or to the RSH pre-defined service (which listens on TCP port number 514).

FortiOS automatically invokes the rsh session helper to process all RSH sessions on TCP port 514. The rsh session helper opens ports required for the RSH service to operate through a FortiGate unit running NAT or transparent and supports port translation of RSH traffic.

Real-Time Streaming Protocol (RTSP) session helper (rtsp)

The Real-Time Streaming Protocol (RTSP) is an application layer protocol often used by SIP to control the delivery of multiple synchronized multimedia streams, for example, related audio and video streams. Although RTSP is capable of delivering the data streams itself it is usually used like a network remote control for multimedia servers. The protocol is intended for selecting delivery channels (like UDP, multicast UDP, and TCP) and for selecting a delivery mechanism based on the Real-Time Protocol (RTP). RTSP may also use the SIP Session Description Protocol (SDP) as a means of providing information to clients for aggregate control of a presentation consisting of streams from one or more servers, and non-aggregate control of a presentation consisting of multiple streams from a single server.

To accept RTSP sessions you must add a security policy with service set to any or to the RTSP pre-defined service (which listens on TCP ports 554, 770, and 8554 and on UDP port 554). The rtsp session helper listens on TCP ports 554, 770, and 8554.

The rtsp session help is required because RTSP uses dynamically assigned port numbers that are communicated in the packet body when end points establish a control connection. The session helper keeps track of the port numbers and opens pinholes as required. In Network Address Translation (NAT) mode, the session helper translates IP addresses and port numbers as necessary.

In a typical RTSP session the client starts the session (for example, when the user selects the Play button on a media player application) and establishes a TCP connection to the RTSP server on port 554. The client then sends an OPTIONS message to find out what audio and video features the server supports. The server responds to the OPTIONS message by specifying the name and version of the server, and a session identifier, for example, 24256-1.

The client then sends the DESCRIBE message with the URL of the actual media file the client wants to play. The server responds to the DESCRIBE message with a description of the media in the form of SDP code. The client then sends the SETUP message, which specifies the transport mechanisms acceptable to the client for streamed media, for example RTP/RTCP or RDT, and the ports on which it receives the media.

In a NAT configuration the rtsp session helper keeps track of these ports and addresses translates them as necessary. The server responds to the SETUP message and selects one of the transport protocols. When both client and server agree on a mechanism for media transport the client sends the PLAY message, and the server begins streaming the media.

Session Initiation Protocol (SIP) session helper (sip)

The sip session helper is described in "The SIP session helper" on page 2507.

Trivial File Transfer Protocol (TFTP) session helper (tftp)

To accept TFTP sessions you must add a security policy with service set to any or to the TFTP pre-defined service (which listens on UDP port number 69). The TFTP session helper also listens on UTP port number 69.

TFTP initiates transfers on UDP port 69, but the actual data transfer ports are selected by the server and client during initialization of the connection. The tftp session helper reads the transfer ports selected by the TFTP client and server during negotiation and opens these ports on the firewall so that the TFTP data transfer can be completed. When the transfer is complete the tftp session helper closes the open ports.

Oracle TNS listener session helper (tns)

The Oracle Transparent Network Substrate (TNS) listener listens on port TCP port 1521 for network requests to be passed to a database instance. The Oracle TNS listener session helper (tns) listens for TNS sessions on TCP port 1521. TNS is a foundation technology built into the Oracle Net foundation layer and used by SQLNET.

Index

D

E

F

G

H

I

K

R

S

T

U

V